COMPUTING p-ADIC L-FUNCTIONS OF TOTALLY REAL NUMBER FIELDS

XAVIER-FRANÇOIS ROBLOT

Abstract. We prove explicit formulas for the p-adic L-functions of totally real number fields and show how these formulas can be used to compute values and representations of p-adic L-functions.

1. Introduction

The aim of this article is to present a general method for computing values and representations of p-adic L-functions of totally real number fields.[1] These functions are the p-adic analogues of the "classical" complex L-functions and are related to those by the fact that they agree, once the Euler factors at p have been removed from the complex L-functions, at negative integers in some suitable congruence classes. The existence of p-adic L-functions was first established in 1964 by Kubota-Leopoldt [22] over $\mathbb{Q}$ and consequently over abelian extensions of $\mathbb{Q}$. It was proved in full generality, 15 years later, by Deligne-Ribet [12] and, independently, by Barsky [3] and Cassou-Noguès [7]. The interested reader can find a summary of the history of their discovery in [7].

There have already appeared many works on the computation of p-adic L-functions, starting with Iwasawa-Sims [20] in 1965 (although they are not explicitly mentioned in the paper) to the more recent computational study of their zeroes by Ernvall-Metsänkylä [16, 17] in the mid-1990's and the current work of Ellenberg-Jain-Venkatesh [15] that provides a conjectural model for the behavior of the λ-invariant of p-adic L-functions in terms of properties of p-adic random matrices. However, most of these articles deal only with L-functions over $\mathbb{Q}$ or that can be written as a product of such L-functions. One remarkable exception is the work of Cartier-Roy [6] in 1972 where computations were carried on to support the existence (at the time not yet proven) of p-adic L-functions over some non-abelian fields of degree 3, 4 and 5.

The method for computing p-adic L-functions given in the present paper is derived from the construction found in [7, 21, 23]. It generalizes a previous work with Solomon [27]. The idea is the following. First, using Shitani's cone decomposition (see Subsection 3.3), we express L-functions in terms of cone zeta functions (see Subsection 3.4, Proposition 3.1 and Equation 3.6). Then, for a given cone zeta function, its values at negative integers are encoded into a power series (see Subsections 3.4 and 3.5). Using the method of Section 2, this power series is then interpreted as a p-adic measure. The p-adic cone zeta function is obtained by integrating suitable p-adic continuous functions against this measure (see Theorem 2.9) once it is proved that it satisfies the required properties (see Subsection 4.1). The main tool for the computation is an explicit formula for the power series associated with the cone zeta function, up to a given precision; see Theorem 4.1. From this formula we give an explicit expression for the values of the cone zeta function at some p-adic integer (Theorem 5.28) and an explicit expression for the corresponding Iwasawa power series (Theorem 5.24). Note that these also are valid only up to a given precision.

Date: October 4, 2011 (draft v.4).

Supported in part by the ANR `AlgoL` (ANR-07-BLAN-0248) and the JSPS Global COE *CompView*.

[1] One can prove that p-adic L-functions of non-totally real number fields are identically zero.

One shortcoming of our method is that it is not very efficient compared to the complex case (see Subsection 5.5 for some complexity estimates). For example, in this simplest case of p-adic L-functions over $\mathbb{Q}$, for a Dirichlet character of conductor f, the complexity in f of the method presented here is $O(f^{1+\epsilon})$, whereas there exist methods to compute complex Dirichlet L-functions in $O(f^{1/2+\epsilon})$. Even in this simple case it remains an open problem whether methods as efficient exist in the p-adic case.

Note. The construction presented in this paper was developed over several years and during that time was used in two previous works; see [5, 28]. It is worth noting that the method has evolved and therefore the brief description of it in these earlier articles does not necessarily match exactly the one that is finally presented here.

Acknowledgments. I would like to express my gratitude to D. Solomon for his invaluable help with this project and for introducing me to the fascinating world of p-adic L-functions. I am also grateful to D. Barsky for his help at the start of the project and to R. de Jeu and A. Weiss for providing with the motivation to complete this project. Finally, I thank heartily D. Ford for reading carefully the earlier version of this article and for his many corrections and helpful comments.

2. p-ADIC INTERPOLATION

Let p be a prime number. Denote by $\mathbb{Q}_p$ the field of rational p-adic numbers. The subring of p-adic integers is denoted by $\mathbb{Z}_p$, and $\mathbb{C}_p$ is the completion of the algebraic closure of $\mathbb{Q}_p$. Let $|\cdot|_p$ denote the p-adic absolute value of $\mathbb{C}_p$ normalized so that $|p|_p = p^{-1}$ and $v_p(.)$ the corresponding valuation; thus $v_p(p) = 1$. For $f \geq 1$, an integer, let W_f denote the subgroup of f-th roots of unity in $\mathbb{C}_p$. The torsion part T_p of the group $\mathbb{Z}_p^\times$ of units in $\mathbb{Z}_p$ is equal to $W_{\varphi(q)}$ where $q := 4$ if $p = 2$, $q := p$ if p is odd, and φ is Euler totient function. We have $\mathbb{Z}_p^\times = T_p \times (1 + q\mathbb{Z}_p)$, and the projections $\omega : \mathbb{Z}_p^\times \to T_p$ and $\langle\cdot\rangle : \mathbb{Z}_p^\times \to 1 + q\mathbb{Z}_p^\times$ are such that $x = \omega(x)\langle x\rangle$ for all $x \in \mathbb{Z}_p^\times$. In particular, we have $x \equiv \omega(x) \pmod q$ for all $x \in \mathbb{Z}_p^\times$.

2.1. Continuous p-adic functions.

For $n \in \mathbb{N} := \{0, 1, 2, \dots\}$, the *binomial polynomial* is defined by

$$\binom{x}{n} := \begin{cases} 1 & \text{if } n = 0, \\ \dfrac{x(x-1)\cdots(x-(n-1))}{n!} & \text{otherwise.} \end{cases} \tag{2.1}$$

The binomial polynomial takes integral values on $\mathbb{Z}$, hence, by continuity, it takes p-adic integral values on $\mathbb{Z}_p$. Let f be a function on $\mathbb{Z}_p$ with values in $\mathbb{C}_p$. One can easily construct by induction a sequence $(f_n)_{n\geq 0}$ of elements of $\mathbb{C}_p$ (see Subsection 5.1) such that

$$f(x) = \sum_{n\geq 0} f_n \binom{x}{n} \quad \text{for all } x \in \mathbb{N}. \tag{2.2}$$

(Note that this is in fact a finite sum.) The coefficients f_n's are uniquely defined and are called the *Mahler coefficients* of f. We have the following fundamental result (see [26, §4.2.4]).

Theorem 2.1 (Mahler expansion). *Let f be a function on $\mathbb{Z}_p$ with values in $\mathbb{C}_p$. Then f is continuous on $\mathbb{Z}_p$ if and only if*

$$\lim_{n\to\infty} |f_n|_p = 0.$$

If f is continuous, then the sequence of continuous functions

$$x \mapsto \sum_{n=0}^{N} f_n \binom{x}{n} \tag{2.3}$$

converges uniformly to f. Reciprocally, let $(f_n)_{n\geq 0}$ be a sequence of elements in $\mathbb{C}_p$ converging to zero. Then the sequence of functions in (2.3) *above converges to a continuous function.*

Denote by $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ the set of continuous functions on $\mathbb{Z}_p$ with values in $\mathbb{C}_p$. For $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$, we define the *norm* of f by

$$\|f\|_p := \max_{x \in \mathbb{Z}_p} |f(x)|_p.$$

The norm of f is a finite quantity since $\mathbb{Z}_p$ is compact and in fact, if $(f_n)_{n \geq 0}$ are the Mahler coefficients of f, we have

$$\|f\|_p = \max_{n \geq 0} |f_n|_p. \tag{2.4}$$

2.2. **A family of continuous functions.** We define a family of continuous functions that will be useful later on. For $s \in \mathbb{Z}_p$, we would like to define $x \mapsto x^s$, where x is an p-adic number, in such a way to extend the definition of $x \mapsto x^k$ when $s = k \in \mathbb{Z}$. In general, it is not possible. However, when $x \in 1 + q\mathbb{Z}_p$, one can set

$$x^s := \sum_{n \geq 0} (x-1)^n \binom{s}{n}.$$

The series converges since $|x - 1|_p < 1$, and by Theorem 2.1, the function $s \mapsto x^s$ is continuous.[2] Furthermore, when $s = k \in \mathbb{N}$ we recover the usual definition of x^k by the binomial theorem, and it is easy to see that this function has the expected properties. With that in mind, for $s \in \mathbb{Z}_p$ we define the function ϕ_s in $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ by

$$\phi_s(x) := \begin{cases} 0 & \text{if } x \in p\mathbb{Z}_p, \\ \langle x \rangle^s & \text{if } x \in \mathbb{Z}_p^\times. \end{cases}$$

It it easy to see that ϕ_s is a continuous function and that its restriction to $\mathbb{Z}_p^\times$ is a group homomorphism. We state two results concerning the properties of ϕ_s. The first one follows directly from construction.

Lemma 2.2. *Let k be a integer. Then, for all $x \in 1 + q\mathbb{Z}_p$, we have*

$$\phi_k(x) = x^k. \qquad \square$$

Lemma 2.3. *The map $s \mapsto \phi_s$ from $\mathbb{Z}_p$ to $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ is continuous.*

Proof. Let s, s' in $\mathbb{Z}_p$. If $x \in p\mathbb{Z}_p$, then $\phi_s(x) = \phi_{s'}(x) = 0$. If $x \in \mathbb{Z}_p^\times$, then

$$\begin{aligned} |\phi_s(x) - \phi_{s'}(x)|_p = \left|\langle x \rangle^s \big(1 - \langle x \rangle^{s'-s}\big)\right|_p &= \left| 1 - \sum_{n \geq 0} \binom{s'-s}{n} (x-1)^n \right|_p \\ &\leq |s' - s|_p \left| \frac{(x-1)^n}{n!} \right|_p \leq |s' - s|_p. \qquad \square \end{aligned}$$

2.3. **Integration of p-adic continuous functions.** A *measure* μ on $\mathbb{Z}_p$ is a bounded linear functional on the $\mathbb{C}_p$-vector space $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$. That is, there exists a constant $B > 0$ satisfying

$$|\mu(f)|_p \leq B \, \|f\|_p \quad \text{for all } f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p). \tag{2.5}$$

The smallest possible B is called the *norm* of the measure μ and is denoted $\|\mu\|_p$. With this norm, the set $\mathcal{M}(\mathbb{Z}_p, \mathbb{C}_p)$ of measures on $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ becomes a $\mathbb{C}_p$-Banach space. From now on, we will write

$$\int f(x) \, d\mu(x) := \mu(f).$$

Usually we will drop the x to simplify the notation when the context is clear.

Lemma 2.4. *The function μ is a continuous map from $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ to $\mathbb{Z}_p$.*

[2] Actually, for $p = 2$ we only need $x \in 1 + 2\mathbb{Z}_2$. But in order to have an analytic function it is necessary to assume $x \in 1 + 4\mathbb{Z}_2$; see Subsection 5.2.

Proof. This is clear by (2.5). □

Lemma 2.5. *Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ with Mahler coefficients $(f_n)_{n\geq 0}$. Then we have*

$$\int f \, d\mu = \sum_{n\geq 0} f_n \int \binom{x}{n} \, d\mu. \tag{2.6}$$

Proof. This is clear since $f = \lim\limits_{N\to\infty} \sum\limits_{n=0}^{N} f_n \binom{x}{n}$ and μ is continuous by the previous lemma. □

For $\mu \in \mathcal{M}(\mathbb{Z}_p, \mathbb{C}_p)$ and $g \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$, the measure $g\mu$ is defined, for any $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$, by

$$\int f(x) \, dg\mu(x) := \int f(x) g(x) \, d\mu(x).$$

When $g = \chi_A$, the characteristic function of an open and closed subset A of $\mathbb{Z}_p$, we will use the notation

$$\int_A f \, d\mu := \int f \, d\chi_A\mu.$$

A measure μ is said to have *support in* A if $\mu = \chi_A\mu$. In other words, for all $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ we have

$$\int_A f \, d\mu := \int f \, d\mu.$$

2.4. **Measures and power series.** Let $\mathbb{C}_p[[T]]^{bd}$ be the $\mathbb{C}_p$-algebra of power series whose coefficients are in $\mathbb{C}_p$ and are bounded in absolute value. Let μ be a measure in $\mathcal{M}(\mathbb{Z}_p, \mathbb{C}_p)$. One associates with μ a power series $F_\mu \in \mathbb{C}_p[[T]]^{bd}$ defined by

$$F_\mu(T) := \sum_{n\geq 0} \int \binom{x}{n} \, d\mu(x) \, T^n.$$

Reciprocally, given a power series $F \in \mathbb{C}_p[[T]]^{bd}$ with coefficients F_n $(n \geq 0)$, one associates with F a measure μ_F defined by

$$\sum_{n\geq 0} \int \binom{x}{n} \, d\mu_F(x) := F_n. \tag{2.7}$$

Indeed, by Lemma 2.5, these equations uniquely determine the measure μ_F. These maps define isometric isomorphisms of $\mathbb{C}_p$-Banach space between $\mathcal{M}(\mathbb{Z}_p, \mathbb{C}_p)$ and $\mathbb{C}_p[[T]]^{bd}$ where the norm on $\mathbb{C}_p[[T]]^{bd}$ is defined to be the maximum of the absolute values of the coefficients; see [23, Chap. 4].

Remark 2.6. Another characterization of the correspondence between measures and bounded power series is that the power series F_μ is the unique power series in $\mathbb{C}_p[[T]]^{\mathrm{bd}}$ such that

$$\int (1+t)^x \, d\mu(x) = F_\mu(t) \quad \text{for all } t \in \mathbb{C}_p \text{ such that } |t|_p < 1.$$

The measures corresponding to powers of $1 + T$ form an important class. The result below follows directly from (2.3), Lemma 2.5 and (2.7) (or simply the remark above).

Lemma 2.7. *Let $a \in \mathbb{Z}_p$. Then the measure associated with the power series*

$$(1+T)^a := \sum_{n\geq 0} \binom{a}{n} T^n \tag{2.8}$$

is the Dirac measure at a, that is, the measure μ_a such that

$$\int f \, d\mu_a = f(a)$$

for all $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$. □

2.5. **The interpolation principle.** Let Δ be the linear operator $(1+T)\dfrac{d}{dT}$ acting on $\mathbb{C}_p[[T]]^{bd}$. Let $\mu \in \mathcal{M}(\mathbb{Z}_p, \mathbb{C}_p)$ be a measure. We have

$$\begin{aligned}\Delta F_\mu(T) &= (1+T)\sum_{n\geq 1} n \int \binom{x}{n}\, d\mu \cdot T^{n-1} = \sum_{n\geq 0} \int \left[(n+1)\binom{x}{n+1} + n\binom{x}{n}\right] d\mu \cdot T^n \\ &= \sum_{n\geq 0} \int x \binom{x}{n} d\mu \cdot T^n = F_{x\mu}(T).\end{aligned}$$

Thus we have proved the first part of the result below; the second follows from Remark 2.6.

Lemma 2.8. *Let μ be a measure with associated power series F_μ. Then the measure associated with the power series ΔF_μ is $x\mu$. In particular,*

$$\Delta^k F_\mu(T)_{|T=0} = \int x^k\, d\mu$$

for any integer $k \geq 0$. □

We can now state the main result of this section.

Theorem 2.9. *Let $(a_n)_{n\geq 0}$ be a sequence of elements of $\mathbb{C}_p$. Assume there exists a power series $F \in \mathbb{C}_p[[T]]^{bd}$ such that for all $k \geq 0$ we have*

$$\Delta^k F(T)_{|T=0} = a_k$$

and that the associated measure μ_F has support in $1 + q\mathbb{Z}_p$. Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be defined by

$$f(s) := \int \phi_s(x)\, d\mu_F(x).$$

Then f is a continuous function such that

$$f(k) = a_k \tag{2.9}$$

for all $k \in \mathbb{N}$.

Proof. It is clear from Lemmas 2.3 and 2.4 that f is continuous. For $k \in \mathbb{N}$ we compute

$$\begin{aligned} f(k) &= \int_{1+q\mathbb{Z}_p} \phi_k(x)\, d\mu_F(x) && \text{since } \mu \text{ has support in } 1+q\mathbb{Z}_p \\ &= \int_{1+_q\mathbb{Z}_p} x^k\, d\mu_F && \text{by Lemma 2.2} \\ &= \int x^k\, d\mu_F && \text{since } \mu \text{ has support in } 1+q\mathbb{Z}_p \\ &= \Delta^k F(T)_{|T=0} && \text{by Lemma 2.8} \\ &= a_k. \end{aligned}$$ □

3. Values of zeta functions at negative integers

Let E be a totally real number field of degree d with ring of integers $\mathbb{Z}_E$. We consider E, and all other number fields, as subfields of the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ contained in $\mathbb{C}$. We also fix once and for all an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$. For α in E, we denote by $\alpha^{(i)} \in \mathbb{R}$, $i = 1, \dots, d$, its conjugates. An element $\alpha \in E$ is *totally positive* if $\alpha^{(i)} > 0$ for $i = 0, \dots, d$. We write $\alpha \gg 0$. The subgroup of totally positive numbers in $E^\times$ is denoted E^+ and we let $\mathbb{Z}_E^+ := E^+ \cap \mathbb{Z}_E$ be the set of totally positive algebraic integers in E. Let $\mathcal{N} = \mathcal{N}_{E/\mathbb{Q}}$ denote the absolute norm of the group $I(E)$ of ideals of E. By abuse, for α a non-zero element in E we write $\mathcal{N}(\alpha) := \mathcal{N}(\alpha\mathbb{Z}_E)$. When α is totally positive $\mathcal{N}(\alpha)$ equals the absolute norm of α.

Let $\mathfrak{m} := \mathfrak{f}\mathfrak{z}$ be a *modulus* of E, that is, the formal product of an integral ideal $\mathfrak{f}$ of E (the finite part) and a subset $\mathfrak{z}$ of the set of infinite places of E (the infinite part). We use the notations

$E_\mathfrak{m}$ for the subgroup of elements of E that are congruent (multiplicatively) to 1 modulo $\mathfrak{m}$,

$I_\mathfrak{m}(E)$ for the subgroup of fractional ideals of E that are relatively prime to $\mathfrak{f}$,

$\mathrm{Cl}_\mathfrak{m}(E)$ for the *ray class group of* E *modulo* $\mathfrak{m}$, that is, the quotient of $I_\mathfrak{m}(E)$ by the subgroup of principal ideals generated by elements of $E_\mathfrak{m}$, and

$h_\mathfrak{m}(E)$ for the cardinality of $\mathrm{Cl}_\mathfrak{m}(E)$.

Finally, we set $U_\mathfrak{m}(E) := U(E) \cap E_\mathfrak{m}$ where $U(E)$ is the unit group of E.

3.1. Twisted partial zeta functions.

Let $\mathfrak{a}$ be a fractional ideal of E, relatively prime to $\mathfrak{f}$. The *partial zeta function* is defined, for $s \in \mathbb{C}$ with $\Re(s) > 1$, by

$$Z_\mathfrak{m}(\mathfrak{a}^{-1}; s) := \sum_{\mathfrak{b} \sim_\mathfrak{m} \mathfrak{a}^{-1}} \mathcal{N}(\mathfrak{b})^{-s}$$

where the sum is over all the integral ideals $\mathfrak{b}$ that are in the same class of $\mathrm{Cl}_\mathfrak{m}(E)$ as the inverse of $\mathfrak{a}$. For $\mathfrak{c}$, an ideal of E, relatively prime with $\mathfrak{f}$, the *twisted partial zeta function* is defined, for $\Re(s) > 1$, by

$$Z_\mathfrak{m}(\mathfrak{a}^{-1}, \mathfrak{c}; s) := \mathcal{N}(\mathfrak{c})^{1-s} Z_\mathfrak{m}((\mathfrak{a}\mathfrak{c})^{-1}; s) - Z_\mathfrak{m}(\mathfrak{a}^{-1}; s). \tag{3.1}$$

The partial zeta functions have meromorphic continuation to the complex plane with a simple pole at $s = 1$. Since the partial zeta functions all have the same residue at $s = 1$, they cancel out in (3.1) and the twisted partial zeta functions have analytic continuation to the whole complex plane.

Let χ be a character on the ray class group $\mathrm{Cl}_\mathfrak{m}(E)$, and let $L_\mathfrak{m}(\chi; s)$ be the corresponding Hecke L-function defined, for $\Re(s) > 1$, by

$$L_\mathfrak{m}(\chi; s) := \prod_{\mathfrak{q} \nmid \mathfrak{m}} \left(1 - \chi(\mathfrak{q})\mathcal{N}(\mathfrak{q})^{-s}\right)^{-1} \tag{3.2}$$

where the product is over all the prime ideals of E not dividing the finite part $\mathfrak{f}$ of the modulus $\mathfrak{m}$. The link between Hecke L-functions and partial zeta function provides a way to express the former in terms of twisted partial zeta functions.

Proposition 3.1. *For all* $s \in \mathbb{C}$ *we have*

$$\left(\chi(\mathfrak{c})\mathcal{N}(\mathfrak{c})^{1-s} - 1\right) L_\mathfrak{m}(\chi; s) = \sum_{i=1}^{h_\mathfrak{m}(E)} \bar{\chi}(\mathfrak{a}_i) Z_\mathfrak{m}(\mathfrak{a}_i^{-1}, \mathfrak{c}; s)$$

where the sum is over ideals $\mathfrak{a}_i$ *representing all the classes of* $\mathrm{Cl}_\mathfrak{m}(E)$.

Proof. We have

$$\begin{aligned}\sum_{i=1}^{h_\mathfrak{m}(E)} \bar{\chi}(\mathfrak{a}_i) Z_\mathfrak{m}(\mathfrak{a}_i^{-1}, \mathfrak{c}; s) &= \mathcal{N}(\mathfrak{c})^{1-s} \sum_{i=1}^{h_\mathfrak{m}(E)} \bar{\chi}(\mathfrak{a}_i) Z_\mathfrak{m}((\mathfrak{a}_i\mathfrak{c})^{-1}; s) - \sum_{i=1}^{h_\mathfrak{m}(E)} \bar{\chi}(\mathfrak{a}_i) Z_\mathfrak{m}(\mathfrak{a}_i^{-1}; s) \\ &= \left(\chi(\mathfrak{c})\mathcal{N}(\mathfrak{c})^{1-s} - 1\right) \sum_{i=1}^{h_\mathfrak{m}(E)} \bar{\chi}(\mathfrak{a}_i) Z_\mathfrak{m}(\mathfrak{a}_i^{-1}; s) \\ &= \left(\chi(\mathfrak{c})\mathcal{N}(\mathfrak{c})^{1-s} - 1\right) L_\mathfrak{m}(\chi; s).\end{aligned}$$

□

We now make some important additional hypotheses.

Hypotheses.

(H1) the finite part $\mathfrak{f}$ of the modulus $\mathfrak{m}$ is divisible by q;

(H2) the infinite part $\mathfrak{z}$ of the modulus $\mathfrak{m}$ contains all the infinite (real) places of E;

(H3) $\mathfrak{c}$ is a prime ideal of residual degree 1.

We will denote by c the prime number below $\mathfrak{c}$; therefore $c = \mathcal{N}(\mathfrak{c})$ by (H3).

Remark 3.2. If $\mathfrak{m}$ does not satisfy both (H1) and (H2) we can enlarge the modulus so that it does satisfy these conditions and we can lift χ to a character of the new modulus. Adding all the infinite places to $\mathfrak{z}$ to satisfy (H2) does not actually change the L-function. Replacing $\mathfrak{f}$ by the lcm of $\mathfrak{f}$ and q to satisfy (H1) has the effect of removing the Euler factors of prime ideals above p in (3.2). This is necessary to be able to do the p-adic interpolation. Another way to achieve this would be to drop (H1) and to require instead that only the elements coprime to q are kept in the cone decompositions (see Subsection 3.3). From a computational point of view these two possibilities are basically the same.

Remark 3.3. The construction of Cassou-Noguès [7] additionally requires $\mathfrak{c}$ to be relatively prime to the co-different of E. However, as we will see in the next subsection, this is not actually necessary.

3.2. **Additive characters modulo $\mathfrak{c}$.** An *additive character* modulo $\mathfrak{c}$ is a group homomorphism ξ from the additive group $\mathbb{Z}_E$ to the multiplicative group $\mathbb{C}^\times$ whose kernel contains $\mathfrak{c}$. We denote by $X(\mathfrak{c})$ the set of all these characters.

Lemma 3.4. *$X(\mathfrak{c})$ is a finite group of order c and all elements in $X(\mathfrak{c})$ but the trivial character have kernel $\mathfrak{c}$. Furthermore, for $x \in \mathbb{Z}_E$ we have*

$$\sum_{\xi \in X(\mathfrak{c})} \xi(x) = \begin{cases} c & \text{if } x \in \mathfrak{c}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let χ be a non-trivial character in $X(\mathfrak{c})$. Then $\mathbb{Z}_E/\operatorname{Ker}(\chi)$ is a quotient group of $\mathbb{Z}_E/\mathfrak{c} \cong \mathbb{Z}/c\mathbb{Z}$ and thus ξ is completely determined by its value on 1, which can be an arbitrary non-trivial c-th root of unity. Therefore there are $c-1$ non-trivial characters and each has kernel $\mathfrak{c}$ since the non-trivial c-th roots of unity all have order c. The last statement is the classical orthogonality relation for characters. □

Proposition 3.5. *Let $\mathfrak{a}$ be an integral ideal coprime to $\mathfrak{f}\mathfrak{c}$. Let A be a set of representatives of the elements of $\mathfrak{a} \cap E_\mathfrak{m}$ under the (multiplicative) action of $U_\mathfrak{m}(E)$. Then for $\Re(s) > 1$*

$$Z_\mathfrak{m}(\mathfrak{a}^{-1}, \mathfrak{c}; s) = \mathcal{N}(\mathfrak{a})^s \sum_{\substack{\xi \in X(\mathfrak{c}) \\ \xi \neq 1}} \sum_{\alpha \in A} \xi(\alpha) \mathcal{N}(\alpha)^{-s}. \tag{3.3}$$

Proof. An ideal $\mathfrak{b}$ is equivalent to $\mathfrak{a}^{-1}$ modulo $\mathfrak{m}$ if and only if there exists $\alpha \in E_\mathfrak{m}$ such that $\mathfrak{b} = \alpha\mathfrak{a}^{-1}$. Furthermore, $\mathfrak{b}$ is integral if and only if α belongs to $\mathfrak{a} \cap E_\mathfrak{m}$, and two elements α and α' of $\mathfrak{a} \cap E_\mathfrak{m}$ yield the same ideal $\alpha\mathfrak{a}^{-1} = \alpha'\mathfrak{a}^{-1}$ if and only if there exists a unit $\epsilon \in U_\mathfrak{m}$ such that $\alpha = \epsilon\alpha'$. Therefore there is a one-to-one correspondence between the integral ideals equivalent to $\mathfrak{a}^{-1}$ modulo $\mathfrak{m}$ and the elements of A. Thus we have

$$Z_\mathfrak{m}(\mathfrak{a}^{-1}; s) = \sum_{\alpha \in A} \mathcal{N}(\alpha\mathfrak{a}^{-1})^{-s} = \mathcal{N}(\mathfrak{a})^s \sum_{\alpha \in A} \mathcal{N}(\alpha)^{-s}. \tag{3.4}$$

We now compute

$$Z_\mathfrak{m}(\mathfrak{a}^{-1}, \mathfrak{c}; s) = \mathcal{N}(\mathfrak{c})^{1-s} Z_\mathfrak{m}((\mathfrak{a}\mathfrak{c})^{-1}; s) - Z_\mathfrak{m}(\mathfrak{a}^{-1}; s)$$

$$= \mathcal{N}(\mathfrak{a})^s \Big(\mathcal{N}(\mathfrak{c}) \sum_{\alpha \in A \cap \mathfrak{c}} \mathcal{N}(\alpha)^{-s} - \sum_{\alpha \in A} \mathcal{N}(\alpha)^{-s} \Big)$$

using (3.4) and the fact that $A \cap \mathfrak{c}$ is a set of representatives of $\mathfrak{ac} \cap E_{\mathfrak{m}}$ modulo $U_{\mathfrak{m}}(E)$, since $\mathfrak{a}$ and $\mathfrak{c}$ are coprime. Finally, we obtain the conclusion using Lemma 3.4. □

3.3. **Cone decomposition.** Let $\beta, \lambda_1, \dots, \lambda_g$ be elements in $\mathfrak{a} \cap \mathbb{Z}_E^+$, with $1 \leq g \leq d$, such that the λ_i's are linearly independent. We define the *discrete cone*[3] *with base point* β *and generators* $\lambda_1, \dots, \lambda_g$ as the following subset of $\mathfrak{a} \cap \mathbb{Z}_E^+$:

$$C(\beta; \lambda_1, \dots, \lambda_g) := \Big\{ \beta + \sum_{i=1}^{g} n_i \lambda_i \text{ with } n_i \in \mathbb{N} \text{ for } 1 \leq i \leq g \Big\}. \tag{3.5}$$

Following the work of Shintani [29], we have the following result of Pi. Cassou-Noguès.

Theorem 3.6 (Cassou-Noguès). *There exists a finite family* $\{C_1, \dots, C_m\}$ *of disjoint discrete cones of* E *with base points belonging to* $\mathfrak{a} \cap E_{\mathfrak{m}}$ *and generators belonging to* $(\mathfrak{af} \cap \mathbb{Z}_E^+)$ *such that a set of representatives of* $\mathfrak{a} \cap E_{\mathfrak{m}}$ *under the action of* $U_{\mathfrak{m}}(E)$ *is given by the union* $C_1 \cup \dots \cup C_m$.

Proof. This is essentially [7, Lemma 1]. □

A finite set $\{C_1, \dots, C_m\}$ of cones satisfying Theorem 3.6 is called a *cone decomposition of* $\mathfrak{a}$ *modulo* $\mathfrak{m}$. A cone C is $\mathfrak{c}$*-admissible* if none of its generators belong to $\mathfrak{c}$. A cone decomposition $\{C_1, \dots, C_m\}$ is $\mathfrak{c}$-admissible if all the cones C_i are $\mathfrak{c}$-admissible (see Remark 5.29 on the existence of such a decomposition). From Proposition 3.5, we have, for $\Re(s) > 1$,

$$Z_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; s) = \mathcal{N}(\mathfrak{a})^s \sum_{\substack{\xi \in X(\mathfrak{c}) \\ \xi \neq 1}} \sum_{j=1}^{m} \sum_{\alpha \in C_j} \xi(\alpha) \mathcal{N}(\alpha)^{-s}. \tag{3.6}$$

3.4. **Cone zeta functions.** Let $C := C(\beta; \lambda_1, \dots, \lambda_g)$ be a $\mathfrak{c}$-admissible cone and ξ be a non-trivial element of $X(\mathfrak{c})$. We define the *zeta function of the pair* (C, ξ), for $\Re(s) > 1$, by

$$Z(C, \xi; s) := \sum_{\alpha \in C} \xi(\alpha) \mathcal{N}(\alpha)^{-s}. \tag{3.7}$$

We associate with the same data a power series $F(C, \xi; T_1, \dots, T_d)$ in $\bar{\mathbb{Q}}[[\underline{T}]] := \bar{\mathbb{Q}}[[T_1, \dots, T_d]]$ in the following way. First, for $r \in \mathbb{C}$, we define a power series in $\mathbb{C}[[T]]$ by[4]

$$(1+T)^r := \sum_{n \geq 0} \binom{r}{n} T^n.$$

Then, for $\alpha \in E$, we define the following power series in $\bar{\mathbb{Q}}[[\underline{T}]]$

$$(1+\underline{T})^\alpha := \prod_{i=1}^{d} (1+T_i)^{\alpha^{(i)}}. \tag{3.8}$$

And finally, we set

$$G(C, \xi; \underline{T}) := \frac{\xi(\beta)(1+\underline{T})^\beta}{\prod_{i=1}^{g} (1 - \xi(\lambda_i)(1+\underline{T})^{\lambda_i})}. \tag{3.9}$$

[3] We will say simply *cone*.

[4] This, of course, gives the usual definition when $r \in \mathbb{N}$.

Remark 3.7. From Lemma 3.4 and the fact that C is $\mathfrak{c}$-admissible it follows that $\xi(\lambda_i)$ is a non-trivial c-th root of unity for all i's and thus the constant term of the denominator is non-zero. Therefore $G(C, \xi; \underline{T})$ is indeed a power series. In fact, its constant term is an algebraic integer divisible only by primes above c.

The *cone zeta function* of C (twisted by $\mathfrak{c}$) is defined by

$$Z(C, \mathfrak{c}; s) := \sum_{\substack{\xi \in X(\mathfrak{c}) \\ \xi \neq 1}} Z(C, \xi; s), \tag{3.10}$$

and in a similar way

$$G(C, \mathfrak{c}; T) := \sum_{\substack{\xi \in X(\mathfrak{c}) \\ \xi \neq 1}} G(C, \xi; T). \tag{3.11}$$

Finally, we define the $\underline{\Delta}$-*operator* acting on $\bar{\mathbb{Q}}[[\underline{T}]]$ by

$$\underline{\Delta} := \prod_{i=1}^{d} (1 + T_i) \frac{\partial}{\partial T_i}. \tag{3.12}$$

Theorem 3.8 (Shintani). *The function $Z(C, \mathfrak{c}; s)$ admits an analytic continuation to $\mathbb{C}$, and, for any integer $k \geq 0$, we have*

$$Z(C, \mathfrak{c}; -k) = \underline{\Delta}^k G(C, \mathfrak{c}; \underline{T})_{|\underline{T} = \underline{0}}. \tag{3.13}$$

Proof. We use the following lemma from Colmez [11, Lemma 3.2].

Lemma 3.9. *For $z_1, \ldots, z_d \in \mathbb{R}^+$ let $f(z_1, \ldots, z_d)$ be a C^∞-function such that it and all its derivatives tend to 0 rapidly at infinity. For all $(s_1, \ldots, s_d) \in \mathbb{C}^d$ such that $\Re(s_i) > 0$ for $i = 1, \ldots, d$ define the function*

$$M(f; s_1, \ldots, s_d) := \int_{(\mathbb{R}^{+*})^d} f(z_1, \ldots, z_d) \frac{z_1^{s_1} \cdots z_d^{s_d}}{\Gamma(s_1) \cdots \Gamma(s_d)} \frac{dz_1}{z_1} \cdots \frac{dz_d}{z_d}. \tag{3.14}$$

Then $M(f; \cdot)$ admits an analytic continuation to $\mathbb{C}^d$ and satisfies

$$M(f; -k_1, \ldots, -k_d) = \prod_{i=1}^{d} \left(-\frac{\partial}{\partial z_i} \right)^{k_i} f(z_1, \ldots, z_d)_{|z_1 = \cdots = z_d = 0}$$

for all $(k_1, \ldots, k_d) \in \mathbb{N}^d$. □

Let $\xi \in X(\mathfrak{c})$ with $\xi \neq 1$. We define a function f_ξ by

$$f_\xi(z_1, \ldots, z_d) := G(C, \xi; e^{-z_1} - 1, \ldots, e^{-z_d} - 1) = \frac{\xi(\beta) e^{-T_{\underline{z}}(\beta)}}{\prod_{i=1}^{g} \left(1 - \xi(\lambda_i) e^{-T_{\underline{z}}(\lambda_i)}\right)} \tag{3.15}$$

where, for $\alpha \in \mathbb{Z}_E$ and $\underline{z} := (z_1, \ldots, z_d) \in \mathbb{C}^d$, we set $T_{\underline{z}}(\alpha) := z_1 \alpha^{(1)} + \cdots + z_d \alpha^{(d)}$. It is clear that this function satisfies the hypothesis of the lemma. Furthermore, for $\underline{z} \in (\mathbb{R}^{+*})^n$ and $\alpha \gg 0$ we have $0 < e^{-T_{\underline{z}}(\alpha)} < 1$, and therefore, by expanding the numerator and by (3.5),

$$f_\xi(z_1, \ldots, z_d) = \sum_{\underline{n} \in \mathbb{N}^g} \xi(\beta + n_1 \lambda_1 + \cdots + n_g \lambda_g) e^{-T_{\underline{z}}(\beta + n_1 \lambda_1 + \cdots + n_g \lambda_g)} = \sum_{\alpha \in C} \xi(\alpha) e^{-T_{\underline{z}}(\alpha)}.$$

Thus we find that

$$M(f_\xi; s_1, \ldots, s_d) = \sum_{\alpha \in C} \xi(\alpha) \int_{\mathbb{R}^{+*}} e^{-z_1 \alpha^{(1)}} \frac{z_1^{s_1}}{\Gamma(s_1)} \frac{dz_1}{z_1} \cdots \int_{\mathbb{R}^{+*}} e^{-z_d \alpha^{(d)}} \frac{z_d^{s_d}}{\Gamma(s_d)} \frac{dz_d}{z_d}.$$

Since

$$\int_{\mathbb{R}^{+*}} e^{-za} z^s \frac{dz}{z} = \Gamma(s)\, a^{-s}$$

for $a \in \mathbb{R}^{+*}$, it follows that

$$M(f_\xi; s, \dots, s) = \sum_{\alpha \in C} \xi(\alpha)(\alpha^{(1)})^s \cdots (\alpha^{(d)})^s = Z(C, \xi; s)$$

for $\Re(s) > 1$. Lastly, we find that

$$-\frac{\partial}{\partial z_i} f_\xi(z_1, \dots, z_d) = \Big((1+T_i)\frac{\partial}{\partial T_i} G\Big)(C, \xi; e^{-z_1} - 1, \dots, e^{-z_d} - 1)$$

for all i's. The conclusion now follows from the lemma, (3.10), and (3.11). □

Recall that we have embedded $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$. Thus we can see $G(C, \mathfrak{c}; \underline{T})$ as having coefficients in $\mathbb{C}_p$ and, generalizing what we did in the first part to higher dimensions, we can try to interpret $G(C, \mathfrak{c}; \underline{T})$ as a measure over $\mathbb{Z}_p^d$. There are two problems. First, the power series $G(C, \mathfrak{c}; \underline{T})$ having several variables complicates things, at least from a computational point of view; it would be much easier to deal with a *one-variable* power series.[5] Second, this power series might not have bounded coefficients, since $\binom{\beta}{n}$ has arbitrarily large p-adic absolute value when β is not a rational p-adic integer. This problem can be solved by making a change of variable in $G(C, \mathfrak{c}; \underline{T})$, as in [30], to transform it into a power series with bounded coefficients. In the next subsection we will see how to transform the power series $G(C, \mathfrak{c}; \underline{T})$ into a one-variable power series satisfying the direct analog of Theorem 3.8. It will turn out that this power series has p-adic integral coefficients, thus solving both problems at the same time.

3.5. **The $\boldsymbol{\Omega}$ operator.** We now explain how to construct an operator that sends $G(C, \mathfrak{c}; \underline{T})$ to an one-variable power series satisfying properties analogous to that of Theorem 3.8. From the definition of $\underline{\Delta}$, we see that Ω should satisfy

$$\Omega((1+T_1)^{a_1} \cdots (1+T_d)^{a_d}) = (1+T)^{a_1 \cdots a_d}.$$

Writing $T_i^{a_i} = ((1+T_i) - 1)^{a_i}$ and developing, we get the following formal definition. Let Ω be the linear function from $\mathbb{C}[\underline{T}]$ to $\mathbb{C}[T]$ defined for $(a_1, \dots, a_d) \in \mathbb{N}^d$ by

$$\Omega(T_1^{a_1} \cdots T_d^{a_d}) := (-1)^{a_1 + \cdots + a_d} \sum_{n_1=0}^{a_1} \cdots \sum_{n_d=0}^{a_d} \Big(\prod_{i=1}^{d} (-1)^{n_i} \binom{a_i}{n_i}\Big) (1+T)^{n_1 \cdots n_d}.$$

The lemma below establishes that this application can be continuously extended to an application from $\mathbb{C}[[\underline{T}]]$ to $\mathbb{C}[[T]]$.

Lemma 3.10. *Let $(a_1, \dots, a_d) \in \mathbb{N}^d$. Then, $\Omega(T_1^{a_1} \cdots T_d^{a_d})$ is divisible by $T^{\max(a_1, \dots, a_d)}$.*

Proof. Assume without loss of generality that a_d is the largest of the a_i's. We have

$$\begin{aligned}\Omega(T_1^{a_1} \cdots T_d^{a_d}) &= (-1)^{a_1 + \cdots + a_{d-1}} \sum_{n_1=0}^{a_1} \cdots \sum_{n_{d-1}=0}^{a_{d-1}} (-1)^{n_1 + \cdots + n_{d-1}} \binom{a_1}{n_1} \cdots \binom{a_{d-1}}{n_{d-1}} \\ &\qquad \times \sum_{n_d=0}^{a_d} (-1)^{a_d - n_d} \binom{a_d}{n_d} \big((1+T)^{n_1 \cdots n_{d-1}}\big)^{n_d} \\ &= (-1)^{a_1 + \cdots + a_{d-1}} \sum_{n_1=0}^{a_1} \cdots \sum_{n_{d-1}=0}^{a_{d-1}} \Big(\prod_{i=1}^{d-1} (-1)^{n_i} \binom{a_i}{n_i}\Big) \big((1+T)^{n_1 \cdots n_{d-1}} - 1\big)^{a_d}\end{aligned}$$

and every term in this sum is divisible by T^{a_d}. □

[5] This is not a big problem though; in fact the computations done in [27] use two-variable power series.

We now prove the main property of the Ω operator, that is, that it "commutes" with the operator $\underline{\Delta}$.

Proposition 3.11. *For $A \in \mathbb{C}[[\underline{T}]]$ we have*

$$\Omega(\underline{\Delta}(A)) = \Delta(\Omega(A)).$$

Proof. By linearity and the fact that the operators Δ, $\underline{\Delta}$, and Ω are linear and continuous,[6] it is enough to prove the result for monomials $T_1^{a_1} \cdots T_d^{a_d}$ with $(a_1, \ldots, a_d) \in \mathbb{N}^d$. But any such monomial can be written as a finite linear combination of $(1+T_1)^{b_1} \cdots (1+T_d)^{b_d}$ with $(b_1, \ldots, b_d)^d \in \mathbb{N}$, for which the result is direct by construction. □

Let C be a $\mathfrak{c}$-admissible cone. We set

$$F(C, \mathfrak{c}; T) := \Omega(G(C, \mathfrak{c}; \underline{T})).$$

Using Proposition 3.11, the next result is a direct consequence of Theorem 3.8.

Theorem 3.12. *For any integer $k \geq 0$ we have*

$$Z(C, \mathfrak{c}; -k) = \Delta^k F(C, \mathfrak{c}; T)_{|T=0}. \qquad \square$$

Let $\mathcal{D} := \{C_1, \ldots, C_m\}$ be a $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$. We define

$$F_{\mathfrak{m}}(\mathfrak{a}, \mathfrak{c}; T) := \sum_{j=1}^{m} F(C_j, \mathfrak{c}; T). \tag{3.16}$$

Corollary 3.13. *For any integer $k \geq 0$ we have*

$$Z_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; -k) = \mathcal{N}(\mathfrak{a})^{-k} \Delta^k F_{\mathfrak{m}}(\mathfrak{a}, \mathfrak{c}; T)_{|T=0}. \tag{3.17}$$

Proof. Clear from (3.6). □

To conclude this subsection, we prove that the power series $F_{\mathfrak{m}}(\mathfrak{a}, \mathfrak{c}; T)$ does not depend on the choice of the cone decomposition $\mathcal{D}$. Indeed, the previous corollary prescribes the values of $\Delta^k F_{\mathfrak{m}}(\mathfrak{a}, \mathfrak{c}; T)_{|T=0}$ for all $k \geq 0$ which, using the following result, ensures the unicity of $F_{\mathfrak{m}}(\mathfrak{a}, \mathfrak{c}; T)$.

Lemma 3.14. *Let $F(T) \in \mathbb{C}[[T]]$ and let $k \geq 0$ be an integer such that $T^k \mid \Delta F(T)$. Then $T^{k+1} \mid F(T) - F(0)$. Furthermore, if $\Delta^k F(T)_{|T=0} = 0$ for all $k \geq 0$ then $F(T) = 0$.*

Proof. Write $F(T) := \sum_{n \geq 0} f_n T^n$. We compute

$$\Delta F(T) = f_1 + \sum_{n \geq 1} \big((n+1) f_{n+1} + n f_n\big) T^n.$$

From this it is easy to see that $T^k \mid \Delta F(T)$ implies $f_1 = \cdots = f_{k+1} = 0$, which proves the first assertion. For the second, let $k \geq 1$. Since $\Delta^k F(T)_{|T=0} = 0$, that is, $T \mid \Delta(\Delta^{k-1} F(T))$, we have $T^2 \mid \Delta^{k-1} F(T)$ by the first part, as $\Delta^{k-1} F(T)_{|T=0}$ by hypothesis. Repeating this process (and using the fact that $F(0) = \Delta^0 F(T)_{|T=0} = 0$), we eventually get $T^{k+1} \mid F(T)$. Since k is arbitrary, it follows that $F(T) = 0$. □

4. p-adic L-functions

We put together the results of the last two sections to construct the p-adic L-functions.

[6] We leave to the reader the verification that Δ and $\underline{\Delta}$ are continuous.

4.1. **Some properties of $F_{\mathfrak{m}}(\mathfrak{a}, \mathfrak{c}; T)$.** Let $\mathfrak{a}$ be an integral ideal coprime to $\mathfrak{c}$ and $\mathfrak{m}$. We prove that the power series $F_{\mathfrak{m}}(\mathfrak{a}, \mathfrak{c}; T)$ possesses the properties required to apply Theorem 2.9. We start by proving a useful expression for $F(C, \xi; T)$ modulo powers of T.

Theorem 4.1. *For integers k and K with $0 \leq k \leq K$ define the rational function*

$$B_{k,K}(x) := (-1)^k \sum_{n=k}^{K} \binom{n}{k} \left(\frac{x}{x-1}\right)^n \in \mathbb{Q}(x). \tag{4.1}$$

Let $C := C(\beta; \lambda_1, \ldots, \lambda_g)$ be a $\mathfrak{c}$-admissible cone and let ξ be a non-trivial element of $X(\mathfrak{c})$. For $N \geq 0$ define the polynomial $F_N(C, \xi; T) \in \mathbb{Q}(\xi)[T]$ by

$$F_N(C, \xi; T) := A(C, \xi) \sum_{k_1, \ldots, k_g = 0}^{(N-1)d} (1 + T)^{\mathcal{N}(\beta + \underline{k} \cdot \underline{\lambda})} \prod_{i=1}^{g} B_{k_i, (N-1)d}(\xi(\lambda_i))$$

where $\underline{k} \cdot \underline{\lambda} := k_1\lambda_1 + \cdots + k_g\lambda_g \in \mathbb{Z}_E$ and

$$A(C, \xi) := \frac{\xi(\beta)}{\prod_{i=1}^{g} (1 - \xi(\lambda_i))}.$$

Then

$$F(C, \xi; T) \equiv F_N(C, \xi; T) \pmod{T^N}.$$

Proof. To simplify the notation we write $a_i := \xi(\lambda_i)/(1 - \xi(\lambda_i))$ and $A := A(C, \xi)$. We compute

$$\begin{aligned} G(C, \xi; \underline{T}) &= \frac{\xi(\beta)(1 + \underline{T})^{\beta}}{\prod_{i=1}^{g} (1 - \xi(\lambda_i)(1 + \underline{T})^{\lambda_i})} = A \frac{(1 + \underline{T})^{\beta}}{\prod_{i=1}^{g} (1 - a_i\, ((1 + \underline{T})^{\lambda_i} - 1))} \\ &= A\, (1 + \underline{T})^{\beta} \sum_{n_1, \ldots, n_g \geq 0} \prod_{i=1}^{g} a_i^{n_i} \left((1 + \underline{T})^{\lambda_i} - 1\right)^{n_i}. \end{aligned}$$

Let $\mathcal{I}$ be the ideal of $\mathbb{C}_p[[\underline{T}]]$ generated by the monomials $T_1^{a_1} \cdots T_d^{a_d}$ where $\max(a_1, \ldots, a_d) \geq N$. For any $P(\underline{T}) \in \mathcal{I}$, it follows by Lemma 3.10 that $\Omega(P) \in T^N \mathbb{C}_p[[T]]$. Furthermore, for $i = 1, \ldots, g$ we have

$$((1 + \underline{T})^{\lambda_i} - 1)^{n_i} \in \mathcal{I} \quad \text{if } n_i \geq (N-1)d + 1.$$

It follows that

$$\begin{aligned} G(C, \xi; \underline{T}) &\equiv A\, (1 + \underline{T})^{\beta} \sum_{n_1, \ldots, n_g = 0}^{(N-1)d} \prod_{i=1}^{g} a_i^{n_i} \left((1 + \underline{T})^{\lambda_i} - 1\right)^{n_i} \\ &\equiv A\, (1 + \underline{T})^{\beta} \sum_{n_1, \ldots, n_g = 0}^{(N-1)d} \prod_{i=1}^{g} \left[a_i^{n_i} \sum_{k_i = 0}^{n_i} (-1)^{n_i - k_i} \binom{n_i}{k_i} (1 + \underline{T})^{k_i\lambda_i} \right] \\ &\equiv A \sum_{k_1, \ldots, k_g = 0}^{(N-1)d} (1 + \underline{T})^{\beta + \underline{k} \cdot \underline{\lambda}} \prod_{i=1}^{g} \sum_{n_i = k_i}^{(N-1)d} (-1)^{n_i - k_i} a_i^{n_i} \binom{n_i}{k_i} \pmod{\mathcal{I}}. \end{aligned}$$

Applying Ω to each side we get

$$F(C, \xi; T) \equiv A \sum_{k_1, \ldots, k_g = 0}^{(N-1)d} (1 + T)^{\mathcal{N}(\beta + \underline{k} \cdot \underline{\lambda})} \prod_{i=1}^{g} B_{k_i, (N-1)d}(\xi(\lambda_i)) \pmod{T^N}. \qquad \square$$

Corollary 4.2. *The power series $F(C, \mathfrak{c}; T)$ has coefficients in $\mathbb{Z}_p$.*

Proof. Let ξ be a non-trivial element of $X(\mathfrak{c})$ and write $C = C(\beta; \lambda_1, \ldots, \lambda_g)$. For $i = 1, \ldots, g$ we know $1 - \xi(\lambda_i)$ is divisible only by primes above c and hence is invertible in $\mathbb{Z}_p[\xi]$. Therefore the polynomials $F_N(C, \xi; T)$ have coefficients in $\mathbb{Z}_p[\xi]$, and it follows from Galois theory (see also Subsection 5.3) that

$$F_N(C, \mathfrak{c}; T) := \sum_{\substack{\xi \in X(\mathfrak{c}) \\ \xi \neq 1}} F_N(C, \xi; T)$$

has coefficients in $\mathbb{Z}_p$. By the theorem we have $F(C, \mathfrak{c}; T) \equiv F_N(C, \mathfrak{c}; T) \pmod{T^N}$ for all $N \geq 0$, and therefore $F(C, \mathfrak{c}; T)$ has coefficients in $\mathbb{Z}_p$. □

Since $F_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; T)$ is the sum of the $F(C_i, \mathfrak{c}; T)$'s where $\{C_1, \ldots, C_m\}$ is a $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$, it follows from the corollary that $F_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; T)$ has coefficients in $\mathbb{Z}_p$. In particular, $F_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; T)$ defines a $\mathbb{Z}_p$-valued measure, which we will denote $\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}$. To be able to apply Theorem 2.9 to this measure we need to prove that $\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}$ has support in $1 + q\mathbb{Z}_p$. We will actually prove a stronger statement that will be useful later. Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Denote by $\mathbb{Q}_0 := \mathbb{Q}$, $\mathbb{Q}_1$, $\mathbb{Q}_2$, … the subfields of $\mathbb{Q}_\infty/\mathbb{Q}$ with $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Let E_∞ be the cyclotomic $\mathbb{Z}_p$-extension of E and let $E_0 := E$, E_1, E_2, … be the subfields of E_∞/E with $\mathrm{Gal}(E_n/E) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Define integers $m_0, m_1 \geq 0$ by $\mathbb{Q}_{m_0} = E \cap \mathbb{Q}_\infty$ and $\mathbb{Q}_{m_0+m_1} = E(\mathfrak{m}) \cap \mathbb{Q}_\infty$. By construction $E_{m_1} = E\,\mathbb{Q}_{m_0+m_1}$ is the intersection of $E(\mathfrak{m})$ and E_∞. The commutative diagram

$$\begin{tikzcd}
\mathrm{Cl}_{\mathfrak{m}}(E) \arrow[r, "\mathcal{N}"] \arrow[d] & (1 + qp^{m_0}\mathbb{Z})/(1 + qp^{m_0+m_1}\mathbb{Z}) \arrow[d] \\
\mathrm{Gal}(E_{m_1}/E) \arrow[r, "\mathrm{res}"] & \mathrm{Gal}(\mathbb{Q}_{m_0+m_1}/\mathbb{Q}_{m_0})
\end{tikzcd} \tag{4.2}$$

comes from Class Field Theory, where the bottom map is the restriction map, the top map is induced by the map $\mathfrak{a} \mapsto \langle \mathcal{N}(\mathfrak{a}) \rangle$, and the vertical maps are the respective Artin maps. Define $e \geq 1$ to be the largest integer such that $W_{p^e} \subset E(W_q)$. It is clear that we have $e = m_0 + v_p(q)$. We note in passing the lemma below, which will be useful later and which is a direct consequence of the diagram.

Lemma 4.3. *For any fractional ideal $\mathfrak{a}$ of E coprime to p we have $\langle \mathcal{N}(\mathfrak{a}) \rangle \in 1 + p^e\mathbb{Z}_p$.* □

We now prove our result on the support of the measure $\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}$.

Proposition 4.4. *The measure $\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}$ has support in $1 + p^{e+m_1}\mathbb{Z}_p$.*

Proof. Let C be a cone in a $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$ and let ξ be a non-trivial element of $X(\mathfrak{c})$. Denote by $\mu_{C,\xi}$, respectively $\mu_{C,\xi}^N$ with $N \geq 1$, the measure associated with the power series $F(C, \xi; T)$, respectively $F_N(C, \xi; T)$, and write $C = C(\beta; \lambda_1, \ldots, \lambda_g)$. For $\underline{k} \in \mathbb{N}^g$ the algebraic integers $\beta + \underline{k} \cdot \underline{\lambda}$, are all congruent to 1 modulo q, and thus we have $\mathcal{N}(\beta + \underline{k} \cdot \underline{\lambda}) \equiv 1 \pmod{q}$. It follows that $\mathcal{N}(\beta + \underline{k} \cdot \underline{\lambda}) = \langle \mathcal{N}(\beta + \underline{k} \cdot \underline{\lambda}) \rangle \in 1 + p^{e+m_1}\mathbb{Z}_p$ by the diagram above, since $\beta + \underline{k} \cdot \underline{\lambda} \in E_{\mathfrak{m}}$. Thus, by Lemma 2.7, the measures $\mu_{\xi,C}^N$ have support in $1 + p^{e+m_1}\mathbb{Z}_p$. The same is true for $\mu_{C,\xi}$ since the measures $\mu_{\xi,C}^N$ converge (weakly) to $\mu_{C,\xi}$. The conclusion follows as well for $\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}$, it being the sum of finitely many such measures. □

Remark 4.5. Replacing $\mathfrak{f}$ by $\mathfrak{f}p^a$ for some $a \geq 1$ does not change the p-adic L-function, as we will see from the interpolation property (4.5) it satisfies (and the unicity statement that follows from it; see Remark 4.11). In particular, by taking a large enough we can force the measures $\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}$ to have support in $1 + p^b\mathbb{Z}_p$ for $b \geq 1$ arbitrarily large. The proposition shows that (H1) is enough to imply that b is already quite large.

4.2. **Construction of p-adic L-functions.** We are now ready to define p-adic L-functions. The first step is to define the p-adic equivalent of twisted partial functions.

Proposition 4.6. *For m an integer and $s \in \mathbb{Z}_p$ define $\mathcal{Z}_{p,\mathfrak{m}}^{(m)}(\mathfrak{a}^{-1}, \mathfrak{c}; s)$ to be the p-adic twisted partial zeta function given by*

$$\mathcal{Z}_{p,\mathfrak{m}}^{(m)}(\mathfrak{a}^{-1}, \mathfrak{c}; s) := \omega(\mathcal{N}(\mathfrak{a}))^m \langle \mathcal{N}(\mathfrak{a}) \rangle^s \int \phi_{-s}(x)\, d\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}. \tag{4.3}$$

Then $\mathcal{Z}_{p,\mathfrak{m}}^{(m)}(\mathfrak{a}^{-1}, \mathfrak{c}; s)$ is a continuous function on $\mathbb{Z}_p$, and

$$\mathcal{Z}_{p,\mathfrak{m}}^{(m)}(\mathfrak{a}^{-1}, \mathfrak{c}; -k) = Z_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; -k)$$

for all $k \in \mathbb{N}$ such that $k + m \equiv 0 \pmod{\varphi(q)}$.

Remark 4.7. Using Proposition 4.4 we could restrict the domain of integration in (4.3) to $1 + p^{e+m_1}\mathbb{Z}_p$ and then replace $\phi_{-s}(x)$ by x^{-s}. This would give a somewhat neater formula, and we will actually use this expression several times in the next subsection. However, from a computational point view it is better to express things as in (4.3), since that is how the computation will actually be done.

Proof. This is a direct application of Theorem 2.9 (changing s to $-s$) with $a_n = Z_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; -n)$ and $F = F_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; T)$, using Corollary 3.13 and Proposition 4.4 and the fact that for $k \in \mathbb{N}$ with $k + m \equiv 0 \pmod{\varphi(q)}$ we have

$$\omega(\mathcal{N}(\mathfrak{a}))^m \langle \mathcal{N}(\mathfrak{a}) \rangle^{-k} = \mathcal{N}(\mathfrak{a})^{-k}. \qquad \square$$

Let χ be a complex character on $\mathrm{Cl}_{\mathfrak{m}}(E)$. Recall that we have embedded $\bar{\mathbb{Q}}$ into $\mathbb{C}_p$ and thus we can view χ also as a p-adic character. Define the character κ of $\mathrm{Cl}_{\mathfrak{m}}(E)$ by the composition

$$\kappa : \mathrm{Cl}_{\mathfrak{m}}(E) \twoheadrightarrow \mathrm{Cl}_q(E) \xrightarrow{\simeq} \mathrm{Gal}(E(q)/E) \longrightarrow (\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\simeq} T_p.$$

The first map is the natural surjection coming from the fact that q divides $\mathfrak{m}$ by (H1). The second sends a class $\mathcal{C}$ to its Artin symbol $\sigma_{\mathcal{C}}$, where $E(q)$ is the ray-class field of E modulo q. The next comes from the fact that $E(q)$ contains the q-th root of unity, and thus we can associate with any $\sigma \in \mathrm{Gal}(E(q)/E)$ a class $\bar{a}$ in $(\mathbb{Z}/q\mathbb{Z})^\times$ such that $\sigma(\zeta) = \zeta^a$ for all $\zeta \in W_q$. The last map sends $\bar{a}$ to $\omega(a) \in T_p$. For a fractional ideal $\mathfrak{a}$ of E, relatively prime to $\mathfrak{m}$, it follows from the definition of the Artin map that $\kappa(\mathfrak{a}) = \omega(\mathcal{N}(\mathfrak{a}))$. As a consequence of the previous result and of Proposition 3.1, we recover the construction of p-adic L-functions.

Theorem 4.8 (Deligne-Ribet, Barsky, Cassou-Noguès)**.** *Let m be an integer, and if $\chi \neq \kappa^{1-m}$ assume further that $\mathfrak{c}$ is such that $\chi(\mathfrak{c}) \neq \kappa^{1-m}(\mathfrak{c})$. Define a p-adic L-function by*

$$L_{p,\mathfrak{m}}^{(m)}(\chi; s) := \left(\frac{\chi(\mathfrak{c})}{\omega(c)^{m-1}\langle c \rangle^{s-1}} - 1 \right)^{-1} \sum_{i=1}^{h_{\mathfrak{m}}(E)} \chi(\mathfrak{a}_i^{-1}) \mathcal{Z}_{p,\mathfrak{m}}^{(m)}(\mathfrak{a}_i^{-1}, \mathfrak{c}; s) \tag{4.4}$$

where the sum is over integral ideals $\mathfrak{a}_i$, relatively prime to $\mathfrak{m}$ and $\mathfrak{c}$, representing all the classes of $\mathrm{Cl}_{\mathfrak{m}}(E)$. Then $L_{p,\mathfrak{m}}^{(m)}(\chi; s)$ is a continuous function on $\mathbb{Z}_p$ (respectively $\mathbb{Z}_p \smallsetminus \{1\}$ if $\chi = \kappa^{1-m}$) and

$$L_{p,\mathfrak{m}}^{(m)}(\chi; -k) = L_{\mathfrak{m}}(\chi; -k) \tag{4.5}$$

for all $k \in \mathbb{N}$ such that $k + m \equiv 0 \pmod{\varphi(q)}$.

Remark 4.9. Assume $\chi\kappa^{m-1}$ is not the trivial character and let N be the Galois closure of $E(\mathfrak{m})/\mathbb{Q}$. Let $\tilde{\sigma} \in \mathrm{Gal}(E(\mathfrak{m})/E)$ be such that $\chi\kappa^{m-1}(\tilde{\sigma}) \neq 1$.[7] Lift $\tilde{\sigma}$ to an arbitrary element σ of $\mathrm{Gal}(N/\mathbb{Q})$. By the theorem of Čebotarev [24, Chap. VIII, Th. 13.4] there exists a positive proportion of prime ideals of N whose Frobenius in $N/\mathbb{Q}$ is σ. Let $\mathfrak{C}$ be one of these prime

[7] We see $\chi\kappa^{m-1}$ as a character on $\mathrm{Gal}(E(\mathfrak{m})/E)$ via the Artin map.

ideals with $\mathfrak{C}$ coprime to $\mathfrak{f}\mathbb{Z}_N$. Then $\mathfrak{c} := \mathfrak{C} \cap \mathbb{Z}_E$ is a prime ideal of E, coprime to $\mathfrak{f}$, of residual degree 1, such that $\chi\kappa^{m-1}(\mathfrak{c}) \neq 1$.

Proof. By the previous result the sum in the RHS of (4.4) is a continuous function on $\mathbb{Z}_p$. We now look at the factor before the sum. It is continuous at $s \in \mathbb{Z}_p$ unless $\chi(\mathfrak{c}) = \omega(c)^{m-1}\langle c\rangle^{s-1}$. Since $\langle c\rangle$ has infinite order, this can happen only for $s = 1$. Thus, $L_{p,\mathfrak{m}}^{(m)}(\chi; s)$ is continuous on $\mathbb{Z}_p \smallsetminus \{1\}$, and also at $s = 1$ if $\chi(\mathfrak{c}) \neq \omega(c)^{1-m}$. We get the first result by noting that $\omega(c) = \kappa(\mathfrak{c})$. For the second, let $k \in \mathbb{N}$ be such that $k + m \equiv 0 \pmod{q}$. The interpolation property follows from Proposition 4.6, Proposition 3.1, and the fact that

$$\frac{\chi(\mathfrak{c})}{\omega(c)^{m-1}\langle c\rangle^{k-1}} = \chi(\mathfrak{c})c^{1-k}. \qquad \square$$

Remark 4.10. Assume $\chi\kappa^{m-1}$ is non-trivial but $\chi\kappa^{m-1}(\mathfrak{c}) = 1$. Then (4.4) still defines a continuous function on $\mathbb{Z}_p \smallsetminus \{1\}$. Moreover, that function is equal to $L_{p,\mathfrak{m}}^{(m)}(\chi; s)$ if $s \neq 1$, and therefore, by continuity, it converges to $L_{p,\mathfrak{m}}^{(m)}(\chi; 1)$ as s tends to 1.

Remark 4.11. Assume p is odd. Then the set $\{-k \text{ with } k \in \mathbb{N} \text{ and } k + m \equiv 0 \pmod{p-1}\}$ is dense in $\mathbb{Z}_p$, and there is a unique continuous p-adic function satisfying (4.5). This proves that $L_{p,\mathfrak{m}}^{(m)}(\chi; s)$ does not depend on the choice of $\mathfrak{c}$. For $p = 2$ the closure of $\{-k \text{ with } k \in \mathbb{N}$ and $k + m \equiv 0 \pmod 2\}$ is either $2\mathbb{Z}_2$ or $1 + 2\mathbb{Z}_2$. Thus (4.5) is not enough to prove unicity. In that case we can use Proposition 4.13 below[8] to conclude that $L_{2,\mathfrak{m}}^{(m)}(\chi; s)$ does not depend on the choice of $\mathfrak{c}$.

There are actually $\varphi(q)$ twisted partial zeta functions or L-functions defined by these two results, depending on the choice of the congruence class of m modulo $\varphi(q)$. However, when χ is the trivial character we see that only for $m \equiv 1 \pmod{\varphi(q)}$ does the corresponding p-adic zeta function possibly have a pole at $s = 1$. (See [11] for the computation of the residue; the fact that it is non-zero is equivalent to the Leopoldt conjecture.) Therefore, *the* p-adic L-function, denoted simply $L_{p,\mathfrak{m}}(\chi; s)$, is defined to be the function corresponding to the choice $m \equiv 1 \pmod{\varphi(q)}$. From now on we will focus uniquely on that case, dropping the exponent in the notation and writing $\mathcal{Z}_{p,\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; s)$ instead of $\mathcal{Z}_{p,\mathfrak{m}}^{(1)}(\mathfrak{a}^{-1}, \mathfrak{c}; s)$, and so on. We will see below (see Proposition 4.14) that the different L-functions for various m can be recovered from $L_{p,\mathfrak{m}}(\chi; s)$ by twisting the character χ by some appropriate power of κ.

4.3. Some properties of p-adic L-functions.

In this subsection we prove some well-known results about p-adic L-functions that will be useful later. The first is a direct consequence of Proposition 4.6 (and the remark that follows it).

Proposition 4.12. *The Mahler expansion of the p-adic twisted partial zeta function is*

$$\mathcal{Z}_{p,\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; s) = \omega(\mathcal{N}(\mathfrak{a})) \sum_{n\geq 0} \int_{1+p^{e+m_1}\mathbb{Z}_p} \left(\langle\mathcal{N}(\mathfrak{a})\rangle x^{-1} - 1\right)^n \, d\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}} \binom{s}{n}. \qquad \square$$

From this, we deduce the analyticity of p-adic L-functions.

Proposition 4.13. *Let $\mathcal{B}_e$ be the open ball in $\mathbb{C}_p$ of center 0 and radius $p^{e-1/(p-1)}$. Then the p-adic L-function $L_{p,\mathfrak{m}}(\chi; s)$ can be extended to an analytic function on $\mathcal{B}_e$, if χ is non-trivial, and to a meromorphic function on $\mathcal{B}_e$ with a pole of order at most 1 at $s = 1$, if χ is trivial.*

Proof. We first prove that the p-adic twisted partial zeta functions $\mathcal{Z}_{p,\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; s)$ can be extended to analytic functions of radius[9] $p^{e-1/(p-1)}$. For $x \in 1 + p^{e+m_1}\mathbb{Z}_p$ it follows from

[8] The proposition only applies to $m \equiv 1 \pmod 2$, but it is straightforward to generalize.

[9] We say that an analytic function has radius r if it converges on the *open* ball in $\mathbb{C}_p$ of center 0 and radius r.

Lemma 4.3 that $\left|\left(\langle\mathcal{N}(\mathfrak{a})x^{-1}\rangle - 1\right)^n\right|_p \leq p^{-en}$, and since the measure $\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}$ is of norm ≤ 1 and $F_{\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; T)$ has coefficients in $\mathbb{Z}_p$ we conclude by the previous proposition that the n-th Malher coefficient of $\mathcal{Z}_{p,\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; s)$ has p-adic absolute value $\leq p^{-en}$. The result then follows from Corollaire 2(c) of [1, p. 162]. (See also Theorem 5.9.)

Denoting by $g(s)$ the inverse of the factor before the sum in the RHS of (4.4) we have

$$g(s) := \chi(\mathfrak{c})\langle c\rangle^{1-s} - 1 = \chi(\mathfrak{c})\ \exp_p((1-s)\log_p\langle c\rangle) - 1$$

where $\exp_p$ and $\log_p$ are respectively the p-adic exponential and logarithm functions (see [26, §5.4]). The function $g(s)$ is analytic on $\mathcal{B}_e$ since $|\log_p\langle c\rangle| \leq q^{-e}$, using again Lemma 4.3 and the fact that the p-adic exponential function has radius $p^{-1/(p-1)}$. Furthermore, from the properties of the p-adic exponential and logarithm functions we see that g has a simple zero at $s = 1$ if $\chi(\mathfrak{c}) = 1$, and does not vanish otherwise. Now if χ is non-trivial we can proceed as in Remark 4.9 and choose $\mathfrak{c}$ such that $\chi(\mathfrak{c}) \neq 1$; this proves the result for the first case. Otherwise we write $g(s) = (s-1)h(s)$ where $h(s)$ is an analytic function non-vanishing on $\mathcal{B}_e$ and the second case follows. □

The next result establishes that the p-adic L-function $L_{p,\mathfrak{m}}^{(m)}(\chi; s)$ for any m in $\mathbb{Z}$ can be recovered from *the* p-adic L-function (corresponding to $m = 1$).

Proposition 4.14. *For any integer m and any $s \in \mathbb{Z}_p$, assuming $s \neq 1$ if $\chi = \kappa^{1-m}$, we have*

$$L_{p,\mathfrak{m}}^{(m)}(\chi; s) = L_{p,\mathfrak{m}}(\chi\kappa^{1-m}; s).$$

Proof. Let $\mathfrak{a}$ be an integral ideal coprime to p. Then $\mathcal{Z}_{p,\mathfrak{m}}^{(m)}(\mathfrak{a}^{-1}, \mathfrak{c}; s) = \kappa(\mathfrak{a})^{m-1}\mathcal{Z}_{p,\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; s)$, since $\kappa(\mathfrak{a}) = \omega(\mathcal{N}(\mathfrak{a}))$, and substitution in (4.4) yields the result. □

A key property of p-adic L-functions is that they are Iwasawa analytic functions (see [25]); we will show this in the proof of the next theorem. Let E_χ be the subextension of $E(\mathfrak{m})/E$ fixed by the kernel of χ. After Greenberg [18] we say that χ is of *type W* if $E_\chi \subset E_\infty$.[10]

Theorem 4.15 (Deligne-Ribet). *Fix a topological generator u of $1 + p^e\mathbb{Z}_p$. Then there exists a unique power series $\mathfrak{I}_{p,\mathfrak{m}}(\chi; X)$ in $\mathbb{Q}_p(\chi)[[X]]$ — or $X^{-1}\,\mathbb{Q}_p(\chi)[[X]]$ if χ is trivial — called the* Iwasawa power series of χ (*with respect to u*) *such that, for all $s \in \mathbb{Z}_p$* (*excepting $s = 0$ if χ is trivial*) *we have*

$$L_{p,\mathfrak{m}}(\chi; 1-s) = \mathfrak{I}_{p,\mathfrak{m}}(\chi; u^s - 1). \tag{4.6}$$

Moreover, if χ is trivial or not of type W then $\mathfrak{I}_{p,\mathfrak{m}}(\chi; X)$ has coefficients in $\mathbb{Z}_p[\chi]$. Otherwise there exists a non-trivial root of unity ξ of order dividing p^{m_1} such that $(\xi(1+X)-1)\mathfrak{I}_{p,\mathfrak{m}}(\chi; X)$ has coefficients in $\mathbb{Z}_p[\chi]$.

Proof. Unicity is clear by (4.6) since the set $\{u^s - 1 \text{ with } s \in \mathbb{Z}_p\} = p^e\mathbb{Z}_p$ admits 0 as a limit point. In particular, if the Iwasawa power series exits it does not depend on the choice of $\mathfrak{c}$. We will use this fact below by choosing prime ideals $\mathfrak{c}$ satisfying additional properties. We now prove existence. For $x \in \mathbb{Z}_p^\times$ with $\langle x\rangle \in 1 + p^e\mathbb{Z}_p$ define

$$\mathcal{L}_u(x) := \frac{\log_p\langle x\rangle}{\log_p u} \in \mathbb{Z}_p,$$

so that

$$\langle x\rangle^s = \left(u^{\mathcal{L}_u(x)}\right)^s = \sum_{\ell\geq 0}(u^s - 1)^\ell\binom{\mathcal{L}_u(x)}{\ell}.$$

[10] See the discussion after Corollary 4.2 for the notation used in the theorem and its proof.

In particular, we can use this equation with $x := \mathcal{N}(\mathfrak{a})$, for some ideal $\mathfrak{a}$ coprime to p, by Lemma 4.3. We define three power series, with coefficients in $\mathbb{Z}_p$, $\mathbb{Z}_p$, and $\mathbb{Z}_p[\chi]$ respectively, as follows.

$$\begin{aligned} N(\mathfrak{a}; X) &:= \mathcal{N}(\mathfrak{a}) \sum_{\ell \geq 0} \binom{-\mathcal{L}_u(\mathcal{N}(\mathfrak{a}))}{\ell} X^\ell = \mathcal{N}(\mathfrak{a})(1+X)^{-\mathcal{L}_u(\mathcal{N}(\mathfrak{a}))}, \\ A(\mathfrak{a}, \mathfrak{c}; X) &:= \sum_{\ell \geq 0} \int_{1+p^{e+m_1}\mathbb{Z}_p} x^{-1} \binom{\mathcal{L}_u(x)}{\ell} \, d\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}} \, X^\ell = \int_{1+p^{e+m_1}\mathbb{Z}_p} x^{-1}(1+X)^{\mathcal{L}_u(x)} \, d\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}, \\ C(\mathfrak{c}, \chi; X) &:= \chi(\mathfrak{c}) \sum_{\ell \geq 0} \binom{\mathcal{L}_u(c)}{\ell} X^\ell - 1 = \chi(\mathfrak{c})(1+X)^{\mathcal{L}_u(c)} - 1. \end{aligned}$$

Then for all $s \in \mathbb{Z}_p$, using (4.3) for the first equality, we have

$$\begin{aligned} N(\mathfrak{a}; u^s - 1)A(\mathfrak{a}, \mathfrak{c}; u^s - 1) &= \mathcal{Z}_{p,\mathfrak{m}}(\mathfrak{a}^{-1}, \mathfrak{c}; 1-s), \\ C(\mathfrak{c}, \chi; u^s - 1) &= \chi(\mathfrak{c})\langle c \rangle^s - 1. \end{aligned}$$

We define

$$\mathfrak{I}_{p,\mathfrak{m}}(\chi; X) := C(\mathfrak{c}, \chi; X)^{-1} \sum_{i=1}^{h_\mathfrak{m}(E)} \chi(\mathfrak{a}_i^{-1}) N(\mathfrak{a}_i; X) A(\mathfrak{a}_i, \mathfrak{c}; X) \tag{4.7}$$

where the sum is over integral ideals $\mathfrak{a}_i$, relatively prime to $\mathfrak{c}$, representing all the classes of $\mathrm{Cl}_\mathfrak{m}(E)$. For all $s \in \mathbb{Z}_p$ such that $C(\mathfrak{c}, \chi; u^s - 1) \neq 0$ it follows from (4.4) and the equalities above that (4.6) holds.

We now consider several cases, not necessarily disjoint. Assume first that the order of χ is not a power of p. We reason as in Remark 4.9 with $\tilde{\sigma} \in \mathrm{Gal}(E(\mathfrak{m})/E)$ such that the order of $\chi(\tilde{\sigma})$ is not a power of p. Then $\chi(\mathfrak{c}) - 1$, the constant coefficient of $C(\mathfrak{c}, \chi; X)$, is a p-adic unit. Therefore $C(\mathfrak{c}, \chi; X)$ does not vanish on $p^e\mathbb{Z}_p$ and is invertible in $\mathbb{Z}_p[\chi][[X]]$. This proves that $\mathfrak{I}_{p,\mathfrak{m}}(\chi; X) \in \mathbb{Z}_p[\chi][[X]]$ and satisfies (4.6) for all $s \in \mathbb{Z}_p$.

Assume now that χ is such that $E_\chi \cap E_\infty = E$. Let N be the Galois closure over $\mathbb{Q}$ of the compositum of E_χ and E_1. Then there exists $\sigma \in \mathrm{Gal}(N/\mathbb{Q})$ such that $\sigma_{|E_\chi}$ is trivial but $\sigma_{|E_1}$ is non-trivial. Let $\mathfrak{C}$ be a prime ideal of N, coprime to $\mathfrak{f}\mathbb{Z}_N$, whose Frobenius is equal to σ, and let $\mathfrak{c} := \mathfrak{C} \cap \mathbb{Z}_E$. Then $\mathfrak{c}$ has residual degree 1, and $\chi(\mathfrak{c}) = 1$ so the constant term of $C(\mathfrak{c}, \chi; X)$ is zero. Also, by construction we have $\mathcal{L}_u(c) \in \mathbb{Z}_p^\times$, and since this is the coefficient of X in $C(\mathfrak{c}, \chi; X)$ it follows that $C(\mathfrak{c}, \chi; X) = XU(X)$, where $U(X) \in \mathbb{Z}_p[\chi][[X]]$ is an invertible power series. Therefore $C(\mathfrak{c}, \chi; X)$ vanishes only at 0, that is, for $s = 0$, and $\mathfrak{I}_{p,\mathfrak{m}}(\chi; X) \in X^{-1}\mathbb{Z}_p[\chi][[X]]$. This proves the result when χ is trivial. When χ is non-trivial, the limit of $\mathfrak{I}_{p,\mathfrak{m}}(\chi; X)$ when $X \to 0$ exists and is finite.[11] Therefore the coefficient of X^{-1} in $\mathfrak{I}_{p,\mathfrak{m}}(\chi; X)$ is zero. This proves the result in the non-trivial case.

Before looking at the other cases we need additional notation and results. Recall that m_0 and m_1 are such that $\mathbb{Q}_{m_0} = E \cap \mathbb{Q}_\infty$ and $\mathbb{Q}_{m_0+m_1} = E(\mathfrak{m}) \cap \mathbb{Q}_\infty$. Let ξ_0 be a root of unity of order p^{m_1}. Define a function on $1 + qp^{m_0}\mathbb{Z}_p$ by

$$a \mapsto \xi_0^{(\log_p a)/(qp^{m_0})}.$$

This map is a group homomorphism with kernel $1 + qp^{m_0+m_1}\mathbb{Z}_p$. Composing with the function on the top in diagram (4.2) we get a character

$$\mathfrak{a} \mapsto \xi_0^{\log_p \langle \mathcal{N}(\mathfrak{a}) \rangle / (qp^{m_0})}$$

on the ray-class group $\mathrm{Cl}_\mathfrak{m}(E)$. It is easy to see from its construction that this character generates the subgroup of characters of $\mathrm{Cl}_\mathfrak{m}(E)$ of type W. Since $e = m_0 + v_p(q)$, we have

[11] It is equal to $L_{p,\mathfrak{m}}(\chi; 1)$.

$\log_p u/(qp^{m_0}) \in \mathbb{Z}_p^\times$ and without loss of generality we can replace ξ_0 by $\xi_0^{\log_p u/(qp^{m_0})}$ to get the character $\rho : \mathfrak{a} \mapsto \xi_0^{\mathcal{L}_u(\mathcal{N}(\mathfrak{a}))}$, which still generates the group of characters of $\mathrm{Cl}_\mathfrak{m}(E)$ of type W. For $v \in \mathbb{Z}$ we compute

$$A(\mathfrak{a}, \mathfrak{c}; \xi_0^v(1+X) - 1) = \int_{1+p^{e+m_1}\mathbb{Z}_p} x^{-1}(\xi_0^v(1+X))^{\mathcal{L}_u(x)}\, d\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}} = A(\mathfrak{a}, \mathfrak{c}; X).$$

We also have $N(\mathfrak{a}; \xi_0^v(1+X) - 1) = \rho^{-v}(\mathfrak{a})N(\mathfrak{a}; X)$ and, for any character ψ of $\mathrm{Cl}_\mathfrak{m}(E)$, $C(\mathfrak{c}, \psi; \xi_0^v(1+X) - 1) = C(\mathfrak{c}, \psi\rho^v; X)$. We conclude that

$$\mathfrak{I}_{p,\mathfrak{m}}(\psi\rho^v; X) = \mathfrak{I}_{p,\mathfrak{m}}(\psi; \xi_0^v(1+X) - 1). \tag{4.8}$$

Assume now that χ is of type W. Then $\chi = \rho^v$ for some $v \in \mathbb{Z}$. Using (4.8) with ψ the trivial character, we find that $(\xi_0^v(1+X) - 1)\mathfrak{I}_{p,\mathfrak{m}}(\chi; X) \in \mathbb{Z}_p[\chi][[X]]$, which proves the result in this case, taking $\xi := \xi_0^v$.

Finally we consider the case $E_\chi \not\subset E_\infty$, in which χ is not of type W and, in particular, $E_\chi \cap E_\infty \neq E$. In this case we can write $\chi = \psi\rho^v$ for some non-trivial character ψ of $\mathrm{Cl}_\mathfrak{m}(E)$ satisfying $E_\psi \cap E_\infty = E$ and some $v \in \mathbb{Z}$. Since the Iwasawa power series for ψ is in $\mathbb{Z}_p[\chi][[X]]$ by the argument above, it follows from (4.8) that the same is true for $\mathfrak{I}_{p,\mathfrak{m}}(\chi; X)$. □

As a first application we use this result to bound the size of the values of p-adic L-functions.

Corollary 4.16. *Let $s \in \mathbb{Z}_p$, with $s \neq 1$ if χ is trivial. Then*

$$|L_{p,\mathfrak{m}}(\chi; s)|_p \le \begin{cases} 1 & \text{if } \chi \text{ is not of type } W, \\ p^{-1/(p-1)} & \text{if } \chi \text{ is of type } W \text{ and non-trivial}, \\ p^e|1-s|_p^{-1} & \text{if } \chi \text{ is trivial.} \end{cases}$$

Proof. The result is clear if χ is not of type W.[12] Assume χ is of type W and non-trivial. In the notation of the theorem we have $v_p(\xi - 1) \le 1/(p-1)$ and $v_p(u^{1-s} - 1) \ge v_p(q)$. From the identity $ab - 1 = (a-1)b + b - 1$ we get $v_p(\xi u^{1-s} - 1) \le 1/(p-1)$ and the result follows. For trivial χ we have $v_p(u^{1-s} - 1) = v_p(1-s) + e$, which proves the result. □

5. Computational methods

In this last section we show how to use the results of the previous sections to compute values and representations of p-adic L-functions explicitly. Note that all computations will involve only p-adic integers — approximated by integers as we explain below — and that we will need to deal with p-adic rational numbers only in the last subsection (and we will do it somewhat indirectly).

In discussing the computation of p-adic approximations we will follow certain terminological conventions. Let $M \ge 1$ be an integer. For $a \in \mathbb{Z}_p$ we denote by $a \bmod p^M$ the unique integer $\tilde{a}$ with $0 \le \tilde{a} < p^M$ such that $|a - \tilde{a}|_p \le p^{-M}$. By "computing a to the precision p^M" we mean computing $a \bmod p^M$. Let L be a finite dimensional $\mathbb{Z}_p$-lattice with $v_1, \ldots, v_n$ a (fixed) basis of L. For $\alpha \in L$, by "computing α to the precision p^M (with respect to the basis $v_1, \ldots, v_n$)" we mean computing the p-adic numbers $a_1, \ldots, a_n$ to the precision p^M, where $\alpha = a_1v_1 + \cdots + a_nv_n$. Note that in what follows the basis $v_1, \ldots, v_n$ is usually not stated explicitly but it should be clear from the context what it is. Let $N \ge 1$ be an integer and let $F(T) \in \mathbb{Z}_p[[T]]$ be a power series. By "computing F to the precision (p^M, T^N)" we mean computing the first N coefficients of F to the precision p^M. Let $\mu \in \mathcal{M}(\mathbb{Z}_p, \mathbb{Z}_p)$ be a measure with values in $\mathbb{Z}_p$. Its associated power series $F_\mu(T)$ must therefore lie in $\mathbb{Z}_p[[T]]$. By "computing μ to the precision (p^M, T^N)" we mean computing the power series F_μ to the precision (p^M, T^N). Finally, let f be a continuous function in $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$. Then its Mahler

[12] In this case we also get the well-known statement: $L_{p,\mathfrak{m}}(\chi; s) \equiv L_{p,\mathfrak{m}}(\chi; 0) \pmod{p^e}$.

coefficients $(f_n)_{n\geq 0}$ are all p-adic integers and tend p-adically to zero. For $M \geq 1$ we denote by $N_f(M)$ the smallest integer $N \geq 0$ such that $|f_n|_p \leq p^{-M}$ for all $n \geq N$. By "computing f to the precision p^M" we mean finding an integer $N \geq N_f(M)$ and computing the coefficients $f_0, \ldots, f_{N-1}$ to the precision p^M.

In the complexity estimates below it is assumed that fast multiplication algorithms are used. Therefore, for example, it takes $O\tilde{~}(M \log p)$ bit operations to multiply two rational p-adic integers to the precision p^M, and it takes $O\tilde{~}(NM \log p)$ bit operations to multiply two power series in $\mathbb{Z}_p[[T]]$ to the precision (p^M, T^N). Here, to simplify the complexity expressions, we have used *$O\tilde{~}$-notation*: $g \in O\tilde{~}(f)$ if there exists $c > 0$ such that $g \in O(f(\log f)^c)$.

Finally, we will assume that the necessary data to work in the field E have been computed. In particular, we assume that an integral basis, say $(\theta_1, \ldots, \theta_d)$, is known. We will express the elements of E with respect to this basis. Also, we assume that the class group, the group of units, and the ray-class group modulo $\mathfrak{m}$ are known. Algorithms to perform these tasks can be found in [8] and [9]; see also [4].

5.1. **Computations with continuous functions.** Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$. For $N \geq 1$, we compute the first N Mahler coefficients of f with the following algorithm.

Algorithm 5.1 (Computation of Mahler coefficients)**.**

```
Input: $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$.
Output: The first $N$ Mahler coefficients of $f$ to the precision $p^M$.
1. For $n = 0$ to $N-1$, do $\tilde{f}_n \leftarrow f(n) \bmod p^M$.
2. For $j = 1$ to $N-1$, for $n = N-1$ to $j$ (decreasing), do $\tilde{f}_n \leftarrow \tilde{f}_n - \tilde{f}_{n-1} \bmod p^M$.
3. Return $\tilde{f}_0, \ldots, \tilde{f}_{N-1}$.
```

Lemma 5.2. *Assume for $x \in \mathbb{Z}_p$ that it takes $O(C)$ bit operations to compute $f(x)$ to the precision p^M. Then Algorithm 5.1 computes the first N Mahler coefficients of f to the precision p^M in $O(NC + N^2 M \log p)$ bit operations. In particular, for $s \in \mathbb{Z}_p$ it takes $O\tilde{~}(NM^2 \log^2 p + N^2 M \log p)$ bit operations to compute the first N Mahler coefficients of ϕ_s to the precision p^M.*

Proof. Let $\tilde{f}_n^{(j)}$ denote the value of $\tilde{f}_n$ after j iterations of the main loop in Step 2. We claim for $0 \leq j \leq N-1$ that

$$\tilde{f}_n^{(j)} = \begin{cases} (\nabla^n f)(0) \mod p^M & \text{for } 0 \leq n \leq j, \\ (\nabla^j f)(n-j) \mod p^M & \text{for } j \leq n \leq N-1, \end{cases}$$

where ∇ is the finite-difference operator defined by $(\nabla f)(s) := f(s+1) - f(s)$. The claim follows for $j = 0$ by the initialization in Step 1 since ∇^0 is the identity. Assume now that the claim holds for some j. If $0 \leq n \leq j$ then $\tilde{f}_n^{(j+1)} = \tilde{f}_n^{(j)}$ and the result is proved. If $n \geq j+1$ then

$$\begin{aligned} \tilde{f}_n^{(j+1)} = \tilde{f}_n^{(j)} - \tilde{f}_{n-1}^{(j)} \mod p^M &= (\nabla^j f)(n-j) - (\nabla^j f)(n-j-1) \mod p^M \\ &= (\nabla(\nabla^j f))(n-j-1) \mod p^M = (\nabla^{j+1} f)(n-(j+1)) \mod p^M \end{aligned}$$

and the result follows by induction. In particular, at the end of the algorithm we have $\tilde{f}_n = (\nabla^n f)(0) \bmod p^M = f_n \bmod p^M$, where $(f_n)_{n\geq 0}$ are the Mahler coefficients of f (see [26, §2.4]). This proves that the algorithm returns the correct result. We now estimate its complexity. The initial step takes $O(NC)$ bit operations by definition and the second step takes $O(N^2 M \log p)$.[13] This proves the first complexity statement.

Now we turn to the computation of $\phi_s(x) \bmod p^M$. We assume s is given by its approximation $s \bmod p^M$, which we will still denote s by abuse. We can also replace x by $x \bmod p^M$

[13] The cost of computing the remainder modulo p^M is also $O(M \log p)$, since $-p^M \leq \tilde{f}_n - \tilde{f}_{n-1} \leq p^M$.

without loss of generality. If p divides x then $\phi_s(x) = 0$. We now suppose that $x \in \mathbb{Z}_p^\times$. For p odd, assume we have computed and stored the values $\omega(a) \bmod p^M$, for $a = 1, \dots, p-1$.[14] Then we can compute $\omega(x) \bmod p^M$ in $O\tilde{~}(M \log p)$ bit operations, since $\omega(x) = \omega(a)$, where $a := x \bmod p$. The computation of $\omega(x)$ for $p = 2$ is trivial. Then $\langle x \rangle = x/\omega(x)$ is computed to the precision p^M in $O\tilde{~}(M \log p)$ bit operations. Assuming fast exponentiation, it takes $O\tilde{~}(M^2 \log^2 p)$ bit operations to compute $\langle x \rangle^s$.[15] Hence it takes $O\tilde{~}(M^2 \log^2 p)$ bit operations to compute the value of $\phi_s(x)$ to the precision p^M. Combining this with the first complexity result completes the proof of the last statement. □

To use the Mahler expansion to compute values of a continuous function we need to compute binomials coefficients $\binom{s}{n}$ to the precision p^M for $n = 0, \dots, N-1$. (We will also need these coefficients for the computation of measures and Iwasawa power series.) We use the following algorithm.

Algorithm 5.3 (Computation of binomial coefficients)**.**

```
**Input:** $s \in \mathbb{Z}_p$.
**Output:** The binomial coefficients $\binom{s}{n}$, for $n = 0, \dots, N-1$, to the precision $p^M$.
**0.** For $n = 1$ to $N$, do $v_n \leftarrow v_p(n)$ and $u_n \leftarrow (np^{-v_n})^{-1} \bmod p^M$.
**1.** Let $V$ be the largest integer $v \geq 0$ such that $p^v \leq N-1$.
   Set $\tilde{s} \leftarrow s \bmod p^{M+V}$.
**2.** Set $A \leftarrow 1$, $B \leftarrow 0$, $b_0 \leftarrow 1$.
**3.** For $n = 1$ to $N-1$, do
       If $\tilde{s} - n + 1 = 0$, set $b_k \leftarrow 0$ for $k = n$ to $N-1$ and go to Step 4.
       $b \leftarrow v_p(\tilde{s} - n + 1)$, $a \leftarrow (\tilde{s} - n + 1)p^{-b} \bmod p^M$,
       $A \leftarrow a u_n A \bmod p^M$, $B \leftarrow B + b - v_n$,
       $b_n \leftarrow Ap^B \bmod p^M$.
**4.** Return $b_0, \dots, b_{N-1}$.
```

Remark 5.4. The precomputations in Step 0 need to be done only once for fixed N and M.

Lemma 5.5. *Algorithm 5.3 computes $\binom{s}{0}, \binom{s}{1}, \dots, \binom{s}{N-1}$ to the precision p^M in $O\tilde{~}(NM \log p)$ bit operations.*

Proof. For $n \geq 0$ and $x \in \mathbb{N}$ define

$$\begin{bmatrix} x \\ n \end{bmatrix} = \begin{cases} 0 & \text{if } \binom{x}{n} = 0, \\ \dbinom{x}{n} p^{-v_p(\binom{x}{n})} & \text{otherwise.} \end{cases}$$

From the recurrence relation satisfied by binomial coefficients it follows that

$$\begin{bmatrix} x \\ n \end{bmatrix} = \frac{(x-n+1)p^{-v_p(x-n+1)}}{np^{-v_p(n)}} \begin{bmatrix} x \\ n-1 \end{bmatrix}.$$

From this one can see by induction that at the end of n-th iteration of the loop in Step 3 we will have $A = \left[\begin{smallmatrix} \tilde{s} \\ n \end{smallmatrix}\right] \bmod p^M$ and $B = v_p(\binom{\tilde{s}}{n})$. Thus the algorithm returns $\binom{\tilde{s}}{n} \bmod p^M$ for $n = 0, \dots, N-1$. Now for $n \geq 1$ we can write $\binom{s}{n} = \frac{s}{n}\binom{s-1}{n-1}$ and therefore

$$\left| \binom{s}{n} \right|_p \leq \frac{|s|_p}{|n|_p}.$$

[14] These can be easily computed using Hensel's Lemma.

[15] For p odd, one could instead compute x^t directly, with t as in the proof of Proposition 5.10.

It follows that $(1+T)^{p^{M+V}} \equiv 1 \pmod{p^M, T^N}$ and thus

$$(1+T)^s \equiv (1+T)^{\tilde{s}} \pmod{p^M, T^N}.$$

Therefore $\binom{s}{n} \equiv \binom{\tilde{s}}{n} \pmod{p^M}$ for $n = 0, \ldots, N-1$, and hence the algorithm returns the correct result.

Lastly we estimate the complexity of the algorithm. For an integer $n \geq 1$ we can compute $v_p(n)$ and $np^{-v_p(n)}$ using $v_p(x) + 1$ divisions by p. Therefore Step 0 performs

$$N + \lfloor N/p \rfloor + \lfloor N/p^2 \rfloor + \cdots \leq N/(p-1)$$

divisions and therefore takes $O\tilde{}(NM \log p)$ bit operations. However, if we use the same method in Step 3 we may end up needing many divisions if $\tilde{s} - n + 1$ has a very large p-adic valuation. A better way to proceed is to use a divide-and-conquer algorithm, so that the computation of a and b can be done in $O(\log(M+V))$ divisions. The computation of A and b_n takes $O\tilde{}(M \log p)$ bit operations, the computation of B is negligible, and, since $V \in O(\log(N))$, Step 3 takes $O\tilde{}(NM \log p)$ bit operations. This completes the proof. □

Remark 5.6. The algorithm can be improved in the following way. In Step 0 and Step 3 we can keep a counter, say `ct`, that we set to p the first time we encounter an integer with a non-zero p-adic valuation. Then at each step we decrease `ct` by 1. If the value of `ct` is non-zero then the p-adic valuation of the corresponding integer is zero. Otherwise we compute the valuation using the method explained above and reset `ct` to the value p. This gains a factor p in computing the p-adic valuation and the prime-to-p part. It does not change the total computation cost estimate however.

Once we have computed sufficiently many Mahler coefficients of f to the precision p^M we can use the algorithm below to compute values of f.

Lemma 5.7. *Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$. Assume we have computed f to the precision p^M with respect to $N \geq N_f(M)$. Then for all $s \in \mathbb{Z}_p$ we can compute $f(s)$ to the precision p^M in $O\tilde{}(NM \log p)$ bit operations.*

Proof. Let $\tilde{f}_0, \ldots, \tilde{f}_{N-1}$ be the first N Mahler coefficients of f to the precision p^M. Then

$$f(s) \equiv \sum_{n=0}^{N-1} \tilde{f}_n \binom{s}{n} \pmod{p^M}.$$

The binomial coefficients are computed using Algorithm 5.3 in $O\tilde{}(NM \log p)$ bit operations, and the computation of the sum also takes $O\tilde{}(NM \log p)$ bit operations. □

Another reason to compute Mahler coefficients is for approximating integrals.

Lemma 5.8. *Let $f \in \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ and let $\mu \in \mathcal{M}(\mathbb{Z}_p, \mathbb{Z}_p)$. Assume we have computed f to the precision p^M with respect to $N \geq N_f(M)$ and have computed μ to the precision (p^M, T^N). Then we can compute $\int f d\mu$ to the precision p^M in $O\tilde{}(NM \log p)$ bit operations.*

Proof. Write $\widetilde{F}_0, \ldots, \widetilde{F}_{N-1}$ (respectively $\tilde{f}_0, \ldots, \tilde{f}_{N-1}$) for the first N coefficients of $F_\mu(T)$ (respectively Mahler coefficients of f) computed to the precision p^M. We have

$$\int f \, d\mu \equiv \sum_{n=0}^{N-1} \tilde{f}_n \widetilde{F}_n \pmod{p^M}.$$

This computation takes $O\tilde{}(NM \log p)$ bit operations. □

From these results it is obvious that having the best possible upper bounds on N_f is crucial for getting the best complexity estimates. In the next subsection we consider this problem for the functions that interest us.

5.2. **Analyticity and Mahler coefficients.** A power series in $\mathbb{C}_p[[X]]$ is *restricted* if its coefficients tend to zero or, equivalently, if it converges on $\mathbb{O}_p := \{x \in \mathbb{C}_p \text{ such that } |x|_p \leq 1\}$. Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be a function. We say f is *analytic* if there exists a restricted power series $\hat{f}(X) \in \mathbb{C}_p[[X]]$ such that

$$f(x) = \hat{f}(x) \qquad \text{for all } x \in \mathbb{Z}_p.$$

For $h \geq 0$ we say f is *locally analytic of order h* if there exist restricted power series $\hat{f}_{a,h}(X)$, with $0 \leq a \leq p^h - 1$, such that

$$f(x) = \hat{f}_{a,h}((x-a)p^{-h}) \qquad \text{for all } x \in a + p^h\mathbb{Z}_p. \tag{5.1}$$

Note that the series $\hat{f}_{a,h}$ are uniquely defined. An analytic function is therefore a locally analytic function of order 0 and one can verify that, if f is analytic of order h_0, then it is analytic of order h for any $h \geq h_0$. Clearly a locally analytic function is continuous. We will see below that the fact that a continuous function is locally analytic has some important consequences for the rate of convergence to zero of its Mahler coefficients.[16] The norm of a restricted power series $\hat{f}$, denoted $\|\hat{f}\|_{p,\infty}$, is defined as the maximum of the absolute values of its coefficients. It can be computed thanks to the following (see [26, Prop. 1, §6.1.4]):

$$\|\hat{f}\|_{p,\infty} = \max_{x \in \mathbb{O}_p^\times} |\hat{f}(x)|_p. \tag{5.2}$$

Let f be a locally analytic function of order h. We define the h-norm of f by

$$M_h(f) := \max_{0 \leq a \leq p^h - 1} \|\hat{f}_{a,h}\|_{p,\infty}.$$

It follows from (5.1) and (5.2) that

$$M_h(f) = \max_{\substack{0 \leq a \leq p^h - 1 \\ x \in \mathbb{O}_p^\times}} |f(a + p^h x)|_p. \tag{5.3}$$

Theorem 5.9 (Amice). *Let f be a function in $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ with Mahler coefficients $(f_n)_{n \geq 0}$. Then f is locally analytic of order h if and only if*

$$\left|\frac{f_n}{\lfloor n/p^h \rfloor !}\right|_p \to 0.$$

Moreover, if f is locally analytic of order h then for all $n \geq 0$ we have

$$|f_n|_p \leq M_h(f)\, \big|\lfloor n/p^h \rfloor !\big|_p.$$

Proof. The first assertion is Corollaire 2(b) of [1, p. 162]. For the second assertion we use the notation and results of Corollaire 1 of [1, p. 157]. Since the sequence $u_n = n$ is very well distributed (*très bien répartie*), it follows from Corollaire 1(c) that

$$v_p(n!/s_{n,h}) = \sum_{k \geq 1} \lfloor n/p^k \rfloor - \sum_{k=1}^{h} \lfloor n/p^k \rfloor = v_p(\lfloor n/p^h \rfloor !).$$

Using Corollaire 1(b), we find that $\left(\lfloor n/p^h \rfloor ! \binom{x}{n}\right)_{n \geq 0}$ is a normal basis (*base normale*) of the Banach space of locally analytic functions of order h. Hence $M_h(f) = \sup_{n \geq 0} |f_n / \lfloor n/p^h \rfloor !|_p$, and the result follows. □

[16] The main reference for these results is the article of Amice [1]; see also [10] for a more accessible presentation.

We are interested in finding optimal upper bounds for N_{ϕ_s}. We remark that the function ϕ_s is locally analytic of order 1 if p is odd and of order 2 if $p = 2$. Indeed, for $x \in a + q\mathbb{Z}_p$ with $a \in \mathbb{Z}_p^\times$ we have

$$\langle x\rangle^s = \langle a\rangle^s \left(\frac{x-a}{a} + 1\right)^s = \langle a\rangle^s \sum_{n\geq 0} \binom{s}{n} \frac{q^n}{a^n} \left(\frac{x-a}{q}\right)^n. \tag{5.4}$$

In this way Theorem 5.9 provides bounds on the Mahler coefficients of ϕ_s. But we can do better with the following result.

Proposition 5.10. *Fix $s \in \mathbb{Z}_p$ and let $(\phi_n)_{n\geq 0}$ be the Mahler coefficients of ϕ_s. Then for all $n \geq 0$ we have*

$$|\phi_n|_p \leq \begin{cases} 2^{-\lfloor n/2\rfloor+1} & \textit{if } p = 2, \\ |n!|_p & \textit{if } p \textit{ is odd.} \end{cases}$$

Remark 5.11. This result is close to optimal for odd p. Indeed, it implies that $|\phi_n/n!|_p \leq 1$ for all $n \geq 0$. On the other hand, we know this quantity is also bounded from below; otherwise Theorem 5.9 would imply that ϕ_s is analytic, and in general it is not.

Proof. Assume p is odd and let B be a positive integer. By the Chinese Remainder Theorem we can find a positive integer t such that

$$\begin{cases} t \equiv s \pmod{p^B}, \\ t \equiv 0 \pmod{p-1}, \\ t \geq B. \end{cases}$$

Then $x^t = \omega(x)^t\langle x\rangle^t \equiv \langle x\rangle^s \pmod{p^B}$ for $x \in \mathbb{Z}_p^\times$ and $x^t \equiv 0 \pmod{p^B}$ for $x \in p\mathbb{Z}_p$. Hence $|\phi_s(x) - x^t|_p \leq p^{-B}$ for all $x \in \mathbb{Z}_p$. It follows from (2.4) and Theorem 5.9 that

$$|\phi_n|_p \leq \max\{|n!|_p,\ p^{-B}\}$$

and we obtain the result by taking B large enough.

For the case $p = 2$ a similar proof works, provided s is even. But for odd s we need to use another approach. So we assume $s \in 1 + 2\mathbb{Z}_2$. Let B and t be positive integers such that $s \equiv t \pmod{2^B}$. As above we have

$$|\phi_s(x) - \omega(x)x^t|_2 \leq 2^{-B} \tag{5.5}$$

where $\omega(x) := 0$ if $x \in 2\mathbb{Z}_2$. We turn now to the computation of bounds on the Mahler coefficients $(a_n)_{n\geq 0}$ of $\omega(x)x^t$. Let i be a fixed square root of -1 in $\bar{\mathbb{Q}}_2$. Then $x \mapsto (\pm i)^x$ are continuous functions[17] on $\mathbb{Z}_2$ and

$$\omega(x) = \frac{i}{2}((-i)^x - i^x) = \frac{i}{2}\sum_{n\geq 0}(i-1)^n(i^n-1)\binom{x}{n}.$$

Thus the Mahler coefficients $(w_n)_{n\geq 0}$ of ω satisfy

$$v_2(w_n) = \begin{cases} +\infty & \text{if } n \equiv 0 \pmod 4, \\ n/2 & \text{if } n \equiv 2 \pmod 4, \\ (n-1)/2 & \text{if } n \equiv 1, 3 \pmod 4. \end{cases}$$

In particular, $v_2(w_n) \geq \lfloor n/2\rfloor$ for all $n \geq 0$. We now apply the following lemma.

[17] But they are not analytic functions.

Lemma 5.12. *Let f and g be two continuous functions with Mahler coefficients $(f_n)_{n\geq 0}$ and $(g_n)_{n\geq 0}$. Then the Mahler coefficients $(c_n)_{n\geq 0}$ of fg satisfy*

$$v_p(c_n) \geq \min_{0\leq k\leq n} \Big(v_p(f_k) + \min_{n-k\leq m\leq n} v_p(g_m) \Big).$$

Proof of the lemma. Let $k, m \geq 0$ be two integers. Then

$$\binom{x}{k}\binom{x}{m} = \sum_{n=\max(k,m)}^{k+m} \nu_n(k,m)\binom{x}{n}$$

for some $\nu_n(k,m) \in \mathbb{Z}$. Hence

$$f(x)g(x) = \sum_{k,m\geq 0} f_k g_m \binom{x}{k}\binom{x}{m} = \sum_{n\geq 0}\left(\sum_{k=0}^{n} f_k \sum_{m=n-k}^{n} g_m\, \nu_n(k,m)\right)\binom{x}{n}$$

and the result follows from the expression of c_n that can be derived from this equality. □

We take $f(x) = \omega(x)$ and $g(x) = x^t$. Then

$$\begin{aligned} v_2(a_n) &\geq \min_{0\leq k\leq n} \Big(v_2(w_k) + \min_{n-k\leq m\leq n} v_2(m!) \Big) = \min_{0\leq k\leq n} \Big(v_2(w_k) + v_2((n-k)!) \Big) \\ &\geq \min_{0\leq k\leq n} (\lfloor k/2 \rfloor + \lfloor (n-k)/2 \rfloor) \geq \lfloor n/2 \rfloor - 1 \end{aligned}$$

and the result follows from this estimate, taking B sufficiently large in (5.5) as before. □

Corollary 5.13. *For every positive integer M we have*

$$N_{\phi_s}(M) \leq \begin{cases} 2M+2 & \text{if } p = 2, \\ pM & \text{if } p \text{ is odd.} \end{cases}$$

Proof. The result is clear for $p = 2$. For p odd, it is enough to prove that the p-adic valuation of $(pM)!$ is at least M. But $v_p((pM)!) = \sum_{k\geq 1} \lfloor pM/p^k \rfloor \geq M$, and the result follows. □

Recall that for $x \in \mathbb{Z}_p^\times$ with $\langle x \rangle \in 1 + p^e\mathbb{Z}_p$ we have set

$$\mathcal{L}_u(x) := \frac{\log_p\langle x \rangle}{\log_p u}$$

where u is a fixed topological generator of $1+p^e\mathbb{Z}_p$. For an integer $\ell \geq 0$ we define a continuous function ψ_ℓ in $\mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p)$ by

$$\psi_\ell(x) := \begin{cases} x^{-1}\dbinom{\mathcal{L}_u(x)}{\ell} & \text{if } \langle x \rangle \in 1 + p^e\mathbb{Z}_p, \\ 0 & \text{otherwise.} \end{cases}$$

We have $x^{-1}(1+S)^{\mathcal{L}_u(x)} = \sum_{\ell\geq 0} \psi_\ell(x) S^\ell$ if $\langle x \rangle \in 1 + p^e\mathbb{Z}_p$. These functions appear in the construction of the Iwasawa power series and will play an important part in their computations.

Proposition 5.14. *The Mahler coefficients $(\psi_{\ell,n})_{n\geq 0}$ of ψ_ℓ satisfy*

$$|\psi_{\ell,n}|_p \leq \frac{|\lfloor n/p^e \rfloor !|_p}{|\ell!|_p}$$

for all $n \geq 0$.

Proof. It is clear that the function ψ_ℓ is locally analytic of order e. The e-norm is $1/|\ell!|_p$, by (5.3). The result follows from Theorem 5.9. □

Corollary 5.15. *For every positive integer M we have*

$$N_{\psi_\ell}(M) \leq p^e(pM + \ell).$$

Proof. It is enough to prove that $v_p((pM + \ell)!) \geq M + v_p(\ell!)$. But this is clear from the facts that $v_p((a + b)!) \geq v_p(a!) + v_p(b!)$ for any two non-negative integers a and b, and that $v_p((pM)!) \geq M$. □

Remark 5.16. This upper bound is in general quite far from optimal. For example, with $p = 3$, $e = 1$, and $\ell = 10$ the corollary gives an upper bound of 210 for $M = 20$, but computations give $N_{\psi_{10}}(20) = 85$. As the complexity of the computation of Iwasawa power series depends heavily upon the size of $N_{\psi_\ell}(M)$ — see for example Theorem 5.24 — it is a good idea to precompute the values $N_{\psi_\ell}(M)$ for small ℓ and M and to use these instead in the computations.

5.3. **Computation of p-adic cone zeta functions.** From (3.16) we see that, once a cone decomposition has been computed,[18] the computation of the p-adic twisted partial zeta functions, and in turn that of the p-adic L-functions, boils down to the computation of p-adic cone zeta functions. We now turn to this computation, but first explaining how to deal with the several zeta functions associated with different additive characters all at once. Define the étale algebra

$$\mathcal{R} := \mathbb{Q}_p[X]/(X^{c-1} + \cdots + 1)$$

and an additive character Ξ from $\mathbb{Z}_E$ to $\mathcal{R}$ by setting

$$\Xi(\alpha) := \eta^a \tag{5.6}$$

for each $\alpha \in \mathbb{Z}_E$, where η is the image of X in $\mathcal{R}$ and a is any positive integer such that $\alpha \equiv a \pmod{\mathfrak{c}}$. The next result is straightforward.

Lemma 5.17. *Let $T_{\mathcal{R}}$ be the trace of $\mathcal{R}/\mathbb{Q}_p$ and let $\alpha \in \mathbb{Z}_E$. Then*

$$T_{\mathcal{R}}(\Xi(\alpha)) = \sum_{\substack{\xi \in X(\mathfrak{c}) \\ \xi \neq 1}} \xi(\alpha).$$ □

Note that $T_{\mathcal{R}}$ is trivial to compute since it is $\mathbb{Q}_p$-linear and we have

$$T_{\mathcal{R}}(\eta^a) = \begin{cases} c - 1 & \text{if } c \mid a, \\ -1 & \text{otherwise.} \end{cases}$$

Let $C := C(\beta; \lambda_1, \ldots, \lambda_g)$ be a $\mathfrak{c}$-admissible cone. For $N \geq 1$ we define

$$F_N(C, \mathfrak{c}; T) := T_{\mathcal{R}}\left[A(C, \Xi) \sum_{k_1,\ldots,k_g=0}^{(N-1)d} (1 + T)^{\mathcal{N}(\beta + \underline{k}\cdot\underline{\lambda})} \prod_{i=1}^{g} B_{k_i,(N-1)d}\big(\Xi(\lambda_i)\big)\right] \tag{5.7}$$

where $A(C, \Xi) := \Xi(\beta)/\prod_{i=1}^{g}(1 - \Xi(\lambda_i))$ and $T_{\mathcal{R}}$ is extended in the natural way to $\mathcal{R}[[T]]$. It follows from Lemma 5.17 and Theorem 4.1 that $F_N(C, \mathfrak{c}; T) \equiv F(C, \mathfrak{c}; T) \pmod{T^N}$. We will use the expression above to compute approximations of $F(C, \mathfrak{c}; T)$ and of its associated measure $\mu_{p,C}^{\mathfrak{c}}$. We define

$$\mathscr{Z}_p(C, \mathfrak{c}; s) := \int \phi_{-s}(x)\, d\mu_{p,C}^{\mathfrak{c}}. \tag{5.8}$$

We now determine some computation costs. These results, or at least their proofs, will be useful later to estimate the complexity of the computation of p-adic L-functions; see Subsection 5.5. The first step is the computation of values of the rational functions $B_{k,K}$.

[18] This will be the topic of the next subsection.

Proposition 5.18. *If K is a non-negative integer then*

$$B_{0,K}(x) = x\left(\frac{x}{x-1}\right)^K - x + 1$$

and for $0 \leq k < K$ we have the recurrence formula

$$B_{k+1,K}(x) = x\left[(-1)^{k+1}\binom{K+1}{k+1}\left(\frac{x}{x-1}\right)^K + B_{k,K}\right].$$

Proof. We first establish another expression for the $B_{k,K}(x)$'s.

Lemma 5.19. *For $k \geq 0$ let Coeff_k denote the linear map that sends a polynomial in $\mathbb{Q}(x)[X]$ to the coefficient of its monomial of degree k. Then*

$$B_{k,K}(x) = \left(\frac{-x}{x-1}\right)^k \mathrm{Coeff}_k\left[\frac{\left(\dfrac{x}{x-1}+X\right)^{K+1} - 1}{\dfrac{1}{x-1}+X}\right].$$

Proof of the lemma. We compute

$$B_{k,K}(x) = \left(\frac{-x}{x-1}\right)^k \sum_{n=k}^{K}\binom{n}{k}\left(\frac{x}{x-1}\right)^{n-k} = \left(\frac{-x}{x-1}\right)^k \sum_{n=k}^{K}\mathrm{Coeff}_k\left[\left(\frac{x}{x-1}+X\right)^n\right]$$

and the conclusion follows by evaluating the sum. □

Now define

$$A_K(X) := \left(\left(\frac{x}{x-1}+X\right)^{K+1} - 1\right)\Big/\left(\frac{1}{x-1}+X\right)$$

and let a_k denote the coefficient of X^k in $A_K(X)$. Then $B_{0,K} = A_K(0)$, which gives the first assertion. Since

$$A_K(X)\left(\frac{1}{x-1}+X\right) = \left(\frac{x}{x-1}+X\right)^{K+1} - 1$$

we see that

$$\frac{a_{k+1}}{x-1} + a_k = \binom{K+1}{k+1}\left(\frac{x}{x-1}\right)^{K-k}$$

for $0 \leq k < K$. The second assertion follows by induction. □

Corollary 5.20. *Let $\alpha \in \mathbb{Z}_E$, coprime with $\mathfrak{c}$, and let $K \geq 1$ be an integer. Then we can compute $B_{0,K}(\Xi(\alpha)), \ldots, B_{K,K}(\Xi(\alpha)) \in \mathcal{R}$ to the precision p^M in $\tilde{O}(KMc\log p + d\log c)$ binary operations.*

Proof. We apply Lemma 5.5 to precompute the binomial coefficients $\binom{K+1}{0}, \ldots, \binom{K+1}{K+1}$ in $\tilde{O}(KM\log p)$ bit operations. Since the prime ideal $\mathfrak{c}$ is of degree 1 there exist integers $t_1, \ldots, t_d \in \{0, \ldots, c-1\}$ such that $\theta_i \equiv t_i \pmod{\mathfrak{c}}$ for $i = 1, \ldots, d$. We assume $t_1, \ldots, t_d$ have been precomputed (using, say, [9, Algo. 1.4.12]). Write $\alpha := a_1\theta_1 + \cdots + a_d\theta_d \in \mathbb{Z}_E$. Then $\alpha \equiv a \pmod{\mathfrak{c}}$, where $a := a_1t_1 + \cdots + a_dt_d \bmod c$ is computed in $\tilde{O}(d\log c)$ bit operations. Next we precompute $(\eta^a/(\eta^a-1))^K$ in $\tilde{O}(Mc\log K\log p)$ bit operations. From this we get $B_{0,K}(\eta^a)$ at negligible additional cost. Then, using the induction formula and the precomputed values, the computation of $B_{k+1,K}(\eta^a)$ from $B_{k,K}(\eta^a)$ takes only $\tilde{O}(Mc\log p)$ bit operations. □

We now can give our first estimate. As we want our results to be valid for several different cones at once, we will express these estimates using d and not g (the number of generators), using the fact that $g \leq d$.

Theorem 5.21. *For any positive integers M and N we can compute the measure $\mu_{p,C}^{\mathfrak{c}}$ to the precision (p^M, T^N) in $\tilde{O}(N^{d+1}d^{d+3}Mc\log p)$ bit operations.*

Proof. We compute $F(C;T)$ using (5.7). Applying the previous proposition we precompute $B_{k,(N-1)d}(\Xi(\lambda_i))$, for $k = 0, \ldots, (N-1)d$ and $i = 1, \ldots, d$, in $\tilde{O}(Nd^2Mc\log p)$ binary operations. With these values precomputed each computation of the inner product in (5.7) takes $\tilde{O}(dMc\log p)$ bit operations. Now let $a := \mathcal{N}(\beta + \underline{k}\cdot\underline{\lambda})$. We compute $(1+T)^a$ to the precision (p^M, T^N), using Lemma 5.5, in $\tilde{O}(NM\log p)$ bit operations, after having computed a to the precision of p^{M+V} (in the notation of Lemma 5.5). The main part of the computation of a is the computation of the norm, which boils down to the computation modulo p^{M+V} of the determinant of a $d\times d$ matrix; see [8, §4.3]. This takes $\tilde{O}(d^3(M+V)\log p)$ bit operations. The multiplication of the power series with the inner product takes $\tilde{O}(NMc\log p)$ bit operations. The sum has $O(N^dd^d)$ terms so the computation of the sum requires $\tilde{O}(N^dd^d(N+d)Mc\log p)$ bit operations. The multiplication by $A(C,\Xi)$ and the computation of the trace take negligible time compared to the computation of the sum. The conclusion follows by putting everything together and simplifying. □

Remark 5.22. It is a good idea to retain the values of $B_{k,K}(\eta^a)$ in order to reuse them if several generators have the same image under Ξ. This does not affect the estimate of the cost of the computation since that estimate is dominated by the cost of computing the sum.

Once the measure $\mu_{p,C}$ has been computed we can use it to compute values of $\mathcal{Z}_p(C,\mathfrak{c};s)$.

Corollary 5.23. *With a precomputation of cost $\tilde{O}(p^{d+1}d^{d+3}M^{d+2}c)$ bit operations, for any given s in $\mathbb{Z}_p$ we can compute $\mathcal{Z}_p(C,\mathfrak{c};s)$ to the precision p^M in $\tilde{O}(p^2M^3)$ bit operations.*

Proof. We use the integral expression (5.8) for $\mathcal{Z}_p(C,\mathfrak{c};s)$. For this we need to compute $\mu_{p,C}^{\mathfrak{c}}$ to the precision (p^M, T^N) with $N > N_f(\phi_s)$. By Corollary 5.13 we can take $N = pM + 2$; the cost of the precomputation comes from the previous theorem. To perform the integration we need to compute the first N $(= pM)$ Mahler coefficients of ϕ_s; by Lemma 5.2 the cost is $\tilde{O}(p^2M^3)$. The cost of computing the integral, as given by Lemma 5.8, is $\tilde{O}(pM^2)$. □

Recall that e is the largest positive integer such that $W_{p^e} \subset E(W_q)$ and that u is a fixed topological generator of $1+p^e\mathbb{Z}_p$. Denote by $\mathfrak{I}_p(C,\mathfrak{c};X)$ the Iwasawa power series of $\mathcal{Z}_p(C,\mathfrak{c};s)$, that is, the (unique) power series in $\mathbb{Z}_p[[X]]$ such that $\mathcal{Z}_p(C,\mathfrak{c};1-s) = \mathfrak{I}_p(C,\mathfrak{c};u^s-1)$ for all $s \in \mathbb{Z}_p$. It is easy to adapt the proof of Theorem 4.15 to show that this power series exists.[19] We now give an explicit formula for $\mathfrak{I}_p(C,\mathfrak{c};X)$ modulo (p^M, X^L).

Theorem 5.24. *Let L and M be positive integers and let $K = (p^e(pM+L)-1)d$. Then*

$$\mathfrak{I}_p(C,\mathfrak{c};X) \equiv$$

$$T_{\mathcal{R}}\Bigg[A(C,\Xi)\sum_{k_1,\ldots,k_g=0}^{K}\mathcal{N}(\beta+\underline{k}\cdot\underline{\lambda})^{-1}(1+X)^{\mathcal{L}_u(\mathcal{N}(\beta+\underline{k}\cdot\underline{\lambda}))}\prod_{i=1}^{g}B_{k_i,K}\big(\Xi(\lambda_i)\big)\Bigg] \pmod{p^M, X^L}.$$

Hence we can compute $\mathfrak{I}_p(C,\mathfrak{c};X)$ to the precision (p^M, X^L) in $\tilde{O}(p^{ed}d^{d+3}(pM+L)^dM^2Lc)$ bit operations.

Proof. We start with a useful lemma.

Lemma 5.25. *Let f be a continuous function on $\mathbb{Z}_p$ with Mahler coefficients $(f_n)_{n\geq 0}$. Let M and N be integers with $M \geq 1$ and $N \geq N_f(M)$. Let μ be a measure of norm ≤ 1. Assume there exist a finite set $\mathcal{A}$ of elements of $\mathbb{Z}_p$ and an element c_a in $\mathbb{O}_p$ for each $a \in \mathcal{A}$ such that*

$$F_\mu(T) \equiv \sum_{a\in\mathcal{A}} c_a(1+T)^a \pmod{T^N}.$$

[19] Actually, the definition of $\mathfrak{I}_p(C,\mathfrak{c};X)$ is given in the proof of the next theorem.

Then

$$\left|\int f\,d\mu - \sum_{a\in\mathcal{A}} c_a f(a)\right|_p \leq p^{-M}.$$

Proof of the lemma. For each $a \in \mathbb{Z}_p$ let δ_a be the Dirac measure at a, and define the measure $\tilde{\mu} := \mu - \sum_{a\in\mathcal{A}} c_a\delta_a$. Then

$$\int g\,d\tilde{\mu} = \int g\,d\mu - \sum_{a\in\mathcal{A}} c_a g(a)$$

for all $g \in \mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$. From this and the facts that $\|\mu\|_p \leq 1$ and $|c_a|_p \leq 1$ for all $a \in \mathcal{A}$ we see that $\tilde{\mu}$ has norm ≤ 1. By Lemma 2.7 the associated power series is divisible by T^N, and thus

$$\left|\int f\,d\tilde{\mu}\right|_p = \left|\sum_{n\geq N} f_n \int \binom{x}{n} d\tilde{\mu}\right|_p \leq \sup_{n\geq N} |f_n|_p \leq p^{-M}. \qquad \square$$

We apply the lemma repeatedly with $\mu = \mu^{\mathfrak{c}}_{p,C}$ and $f = \psi_\ell$ for each $\ell = 0, \ldots, L$ and using (5.7) for the definitions of the set $\mathcal{A}$ and the coefficients c_a. By Corollary 5.15 we can take $N = p^e(pM + L)$. We have

$$\begin{aligned}\mathfrak{I}_p(C,\mathfrak{c};X) &= \sum_{\ell\geq 0}\int \psi_\ell(x)\,d\mu^{\mathfrak{c}}_{p,C}\,X^\ell \equiv \sum_{\ell=0}^{L-1}\int \psi_\ell(x)\,d\mu^{\mathfrak{c}}_{p,C}\,X^\ell \pmod{X^L}\\ &\equiv T_{\mathcal{R}}\left[\sum_{\ell=0}^{L-1} A(C,\Xi)\sum_{k_1,\ldots,k_g=0}^{(N-1)d}\psi_\ell(\mathcal{N}(\beta+\underline{k}\cdot\underline{\lambda}))\prod_{i=1}^{g} B_{k_i,(N-1)d}\big(\Xi(\lambda_i)\big)X^\ell\right] \pmod{p^M, X^L},\end{aligned}$$

the expression for $\mathfrak{I}_p(C,\mathfrak{c};X)$ coming from the fact that $\sum_{\ell=0}^{L-1}\psi_\ell(x)X^\ell \equiv x^{-1}(1+X)^{\mathcal{L}_u(x)} \pmod{X^L}$.

We now estimate the cost of computing $\mathfrak{I}_p(C,\mathfrak{c};X)$ by this formula. As above, precomputation of the $B_{k,K}$'s has a cost of $\tilde{O}(p^{e+1}dM^2Lc)$ binary operations, after which we can compute each inner product in $\tilde{O}(dMc\log p)$ bit operations. The computation of $a := \mathcal{L}_u(\mathcal{N}(\beta+\underline{k}\cdot\underline{\lambda}))$ to the precision p^M takes $\tilde{O}(M(M+e)\log p + d^3(M+V)\log p)$ bit operations.[20] Once the norm has been computed the main computation is that of the p-adic logarithm, which must be done to the precision p^{M+e} since we will be dividing by $\log_p(u) \in p^e\mathbb{Z}_p$. Since $\langle\mathcal{N}(\beta+\underline{k}\cdot\underline{\lambda})\rangle \in 1+p^e\mathbb{Z}_p$ this computation can be done using at most M multiplications of precision p^{M+e}. Computing $(1+X)^a$ to the precision (p^M, X^L) takes $\tilde{O}(ML\log p)$ operations and multiplying by the inner product and the inverse of the norm costs $\tilde{O}(MLc\log p)$ bit operations. The result follows from simplifying and noting that the sum has $O(p^{ed}d^d(pM+L)^d)$ terms.[21] □

Corollary 5.26. *With a precomputation of cost $\tilde{O}(p^{(e+1)d}d^{d+3}M^{d+2}c)$ bit operations, for any given s in $\mathbb{Z}_p$ we can compute $\mathscr{Z}_p(C,\mathfrak{c};s)$ to the precision p^M in $\tilde{O}(M^2\log^2 p)$ bit operations.*

Proof. With $L := \lceil M/e\rceil$ we precompute $\mathfrak{I}_p(C,\mathfrak{c};X)$ to the precision (p^M, X^L), using the theorem to estimate the cost. Given $s \in \mathbb{Z}_p$, we compute $t := u^{1-s} - 1 \in p^e\mathbb{Z}_p$ to the precision p^M in $\tilde{O}(M^2\log^2 p)$ bit operations and compute $\mathfrak{I}_p(C,\mathfrak{c};t) \equiv \mathscr{Z}_p(C,\mathfrak{c};s) \pmod{p^M}$ in $\tilde{O}((M^2/e)\log p)$ operations. The corollary follows. □

Remark 5.27. From its definition it would seem more natural to compute $\mathfrak{I}_p(C,\mathfrak{c};X)$ modulo $(X,p^e)^L$. In particular, it would be enough to compute values of $\mathscr{Z}_p(C,\mathfrak{c};s)$. This implies that, for $0 \leq \ell < L$, the coefficient of X^ℓ would have to be computed to the precision $p^{e(L-\ell)}$. By Corollary 5.15 we can replace $N = p^e(p\lceil L/e\rceil + L)$ with $N = \max_{0\leq\ell<L} p^e(pe(L-\ell) +$

[20] See the proof of Theorem 5.21 for the computation of the norm.

[21] The costs of computing the product by $A(C,\Xi)$ and the trace are negligible compared to that of the sum.

$\ell) = p^{e+1}Le$ in the formula $K = (N-1)d$. It is clear that this does not give a significant improvement in the estimate of the computation time.

We finish this subsection with a result on the direct computation of $\mathcal{Z}_p(C, \mathfrak{c}; s)$ for a given $s \in \mathbb{Z}_p$.

Theorem 5.28. *If $s \in \mathbb{Z}_p$ then*

$$\mathcal{Z}_p(C, \mathfrak{c}; s) \;\equiv\; T_{\mathcal{R}}\left[A(C,\Xi) \sum_{k_1,\ldots,k_g=0}^{(pM+1)d} \mathcal{N}(\beta + \underline{k}\cdot\underline{\lambda})^{-s} \prod_{i=1}^{g} B_{k_i,(pM+1)d}\big(\Xi(\lambda_i)\big)\right] \pmod{p^M}$$

and hence we can compute $\mathcal{Z}(C, \mathfrak{c}; s)$ to the precision p^M in $O\tilde{}(p^d d^{d+3} M^{d+2} c)$ bit operations.

Proof. We use Lemma 5.25 again with $\mu = \mu_{p,C}^{\mathfrak{c}}$ and $f(x) = \phi_{-s}(x)$. By Corollary 5.13 we can take $N = pM + 2$. This establishes the formula. We estimate the computation cost as in Theorem 5.21, replacing the computation of $(1+T)^a$ by that of a^{-s}, with $a := \mathcal{N}(\beta + \underline{k}\cdot\underline{\lambda})$, and accounting for the difference in the number of terms in the sum. □

5.4. **Explicit cone decomposition.** The construction of the measure $\mu_{p,\mathfrak{m}}^{\mathfrak{a},\mathfrak{c}}$ relies on the existence of a cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$. Such a construction exists by a result of Cassou-Noguès [7] (see Theorem 3.6), based on the work of Shintani [29], but the proof is nonconstructive. For $d = 1$ the construction is trivial, and the case $d = 2$ has been well studied (see below). For $d = 3$ an explicit efficient decomposition is given in [13], but quantitative results on the number of discrete cones obtained at the end are missing. A general construction is given in [11], but this construction relies on the existence of a set of units satisfying certain conditions and there does not appear to be any practical way to construct such a set. However, the construction is generalized in [14] for any set of units of maximal rank, at the price of using signed cones rather than cones.[22] This does not cause any complication in the computations and the changes needed to use signed cones are straightforward.

Remark 5.29. The construction given in the present article assumes that we can always find a $\mathfrak{c}$-admissible cone decomposition. Although this is always possible in the case $d = 1$ and $d = 2$ (see below), it is not guaranteed by Theorem 3.6 in general. This is not really a problem however; one can always first construct the several cone decompositions needed, then choose $\mathfrak{c}$ so that these cone decompositions are $\mathfrak{c}$-admissible. This is how it is done in [7].

We start with the case $d = 1$, which is straightforward.

Proposition 5.30. *Assume $d = 1$, that is, $E = \mathbb{Q}$. Let f and a be positive integers such that $\mathfrak{m} = f\mathbb{Z}\cdot\infty$ and $\mathfrak{a} = a\mathbb{Z}$ and let $b = a(a^{-1} \bmod f)$.*[23] *Then a $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$ is given by the unique cone $C(b; af)$.* □

It is also not difficult to construct a cone decomposition in the quadratic case. Indeed, assume $d = 2$; then E is a real quadratic field. For two linearly independent elements γ_0 and γ_1 of E^+ we define the *half-open rational cone of* $\mathfrak{a}$ *modulo* $\mathfrak{m}$ (or simply the *rational cone* of $\mathfrak{a}$ modulo $\mathfrak{m}$) generated by γ_0 and γ_1 to be the following subset of $\mathfrak{a} \cap E^+$:

$$RC_{\mathfrak{m}}(\gamma_0, \gamma_1; \mathfrak{a}) := \{\, s\gamma_0 + t\gamma_1 \text{ with } s, t \in \mathbb{Q},\ 0 < s,\ 0 \le t \,\} \cap \mathfrak{a} \cap E_{\mathfrak{m}}.$$

We go from half-open rational cones to discrete cones using the formula

$$RC_{\mathfrak{m}}(\gamma_0, \gamma_1; \mathfrak{a}) = \bigsqcup_{\alpha \in PC_{\mathfrak{m}}(\gamma_0,\gamma_1;\mathfrak{a})} C(\alpha; \gamma_0, \gamma_1) \quad \text{(disjoint union)} \qquad (5.9)$$

where

$$PC_{\mathfrak{m}}(\gamma_0, \gamma_1; \mathfrak{a}) := \{\, s\gamma_0 + t\gamma_1 \text{ with } s, t \in \mathbb{Q},\ 0 < s \le 1,\ 0 \le t < 1 \,\} \cap \mathfrak{a} \cap E_{\mathfrak{m}}.$$

[22] That is, cones together with a ± sign; the decomposition is obtained by removing the cones with a − sign.

[23] In particular, by (H1), q divides f.

Thus from a finite family of disjoint half-open rational cones giving a set of representatives of $\mathfrak{a}\cap E_{\mathfrak{m}}$ modulo $U_{\mathfrak{m}}(E)$ we can get a $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$, provided that the generators of the rational cones are in $\mathfrak{af}\setminus\mathfrak{c}$. Let ϵ_+ be the generator of $U_+(E)$, the group of totally positive units of E, with $\epsilon_+^{(2)} > 1 > \epsilon_+^{(1)}$. Let $i_{\mathfrak{m}}$ be the index of $U_{\mathfrak{m}}(E)$ as a subgroup of $U_+(E)$; thus $\epsilon_{\mathfrak{m}} := \epsilon_+^{i_{\mathfrak{m}}}$ is a generator of $U_{\mathfrak{m}}(E)$. For any totally positive element γ of $\mathfrak{af}\setminus\mathfrak{c}$ one can easily check that $RC_{\mathfrak{m}}(\gamma,\epsilon_{\mathfrak{m}}\gamma;\mathfrak{a})$ is a set of representatives of $\mathfrak{a}\cap E_{\mathfrak{m}}$ modulo $U_{\mathfrak{m}}(E)$, and therefore we can construct from this rational cone a $\mathfrak{c}$-admissible cone decomposition by the formula above.[24] However, the number of points in $PC_{\mathfrak{m}}(\gamma,\epsilon\gamma;\mathfrak{a})$ is of the order of $\epsilon_{\mathfrak{m}}^{(2)} = (\epsilon_+^{(2)})^{i_{\mathfrak{m}}}$ and therefore much too large for computations in general. We use instead the following algorithm, also used in [27], which is based on the work of Hayes [19]. For two elements γ_0 and γ_1 of E^+ we set

$$b(\gamma_0,\gamma_1) := \lceil \gamma_0^{(1)}/\gamma_1^{(1)} \rceil \quad\text{and}\quad R(\gamma_0,\gamma_1) := -\gamma_0 + b(\gamma_0,\gamma_1)\,\gamma_1.$$

Algorithm 5.31 (Computation of cone decomposition in degree 2).

```
Input: Ideal $\mathfrak{a}$ coprime to $\mathfrak{c}$ and $\mathfrak{m}$.
Output: A $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$.
1. Compute $g \in \mathbb{N}$ and $h \in \mathbb{Z}_E$ such that $\mathfrak{af} = \mathbb{Z}g + \mathbb{Z}h$.
2. If $h^{(2)} < h^{(1)}$ then do $h \leftarrow -h$.
   Do $h \leftarrow h + \lceil -h^{(1)}/g \rceil g$. Set $(g_0, g_1) \leftarrow (g, h)$.
3. While $g_1^{(2)} < g_0^{(2)}$, do $(g_0, g_1) \leftarrow (g_1, R(g_0, g_1))$.
4. If $g_0 \in \mathfrak{c}$ then do $(g_0, g_1) \leftarrow (g_1, R(g_0, g_1))$.
5. Set $D \leftarrow \emptyset$ and $g_{\mathrm{last}} \leftarrow g_0\epsilon_{\mathfrak{m}}$.
6. While $g_0 \neq g_{\mathrm{last}}$, do
  6.1. If $g_1 \notin \mathfrak{c}$ then do
         $b_0 \leftarrow g_0$, $b_1 \leftarrow g_1$ and $(g_0, g_1) \leftarrow (g_1, R(g_0, g_1))$,
       Else
         $g_2 \leftarrow R(g_0, g_1)$,
         $b_0 \leftarrow g_0$, $b_1 \leftarrow g_2$ and $(g_0, g_1) \leftarrow (g_2, R(g_1, g_2))$.
  6.2. For $a \in PC_{\mathfrak{m}}(b_0, b_1; \mathfrak{a})$, do $D \leftarrow D \cup \{C(a; b_0, b_1)\}$.
7. Return $D$.
```

Proposition 5.32. *Let D_E be the discriminant of E and let ϵ_+ be the generator of the group $U_+(E)$ of totally positive units of E such that $\epsilon_+ > 1$.*[25] *Then Algorithm 5.31 computes a $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$ in $O\tilde{}\big(\mathcal{N}(\mathfrak{af})\sqrt{D_E} + \mathcal{N}(\mathfrak{f})^2\,\epsilon_+\log D_E\big)$ operations in E. Moreover, this cone decomposition contains $O\tilde{}\big(\mathcal{N}(\mathfrak{f})\,\epsilon_+\log D_E\big)$ cones.*

Proof. The pair (g,h) constructed in Step 2 of the algorithm satisfies $\mathfrak{af} = \mathbb{Z}g + \mathbb{Z}h$, $g^{(1)} > h^{(1)}$ and $1 < h^{(2)}/h^{(1)}$. From this pair we construct in the following steps a sequence $(\tilde\gamma_n)_{n\geq 0}$ with $(\tilde\gamma_0,\tilde\gamma_1) := (g,h)$ and $\tilde\gamma_{n+1} := R(\tilde\gamma_{n-1},\tilde\gamma_n)$ for $n \geq 1$. One can prove that the elements of this sequence satisfy

$$(1)\ \mathfrak{af} = \mathbb{Z}\tilde\gamma_n + \mathbb{Z}\tilde\gamma_{n+1},\quad (2)\ \tilde\gamma_n^{(1)} > \tilde\gamma_{n+1}^{(1)},\quad\text{and}\quad (3)\ \tilde\gamma_n^{(2)}/\tilde\gamma_n^{(1)} < \tilde\gamma_{n+1}^{(2)}/\tilde\gamma_{n+1}^{(1)}.$$

One can also prove (see below) that there exists an integer $N \geq 1$ such that

$$(4)\ \tilde\gamma_{n-1}^{(2)} < \tilde\gamma_n^{(2)} \quad\text{for all}\quad n \geq N.$$

[24] We will explain below in the proof of the next proposition how to compute the elements of $PC_{\mathfrak{m}}(\gamma_0,\gamma_1;\mathfrak{a})$.

[25] To simplify the expressions, we assume from now on that E is embedded into $\mathbb{R}$ by the map $x \mapsto x^{(2)}$.

We let $\gamma_n := \tilde{\gamma}_{N+n}$ for $n \geq 0$. This is the sequence that is computed after Step 3. The points γ_n are successive points on the *convexity polygon* of $\mathfrak{a}\mathfrak{f}$ as defined in [19]. We can also extend the sequence in the other direction to obtain a sequence $(\gamma_n)_{n\in\mathbb{Z}}$, infinite in both directions, containing all the points on the convexity polygon, and for which we still have $\gamma_{n+1} = R(\gamma_{n-1}, \gamma_n)$ for all $n \in \mathbb{Z}$. It will be necessary to ensure that $\gamma_0 \notin \mathfrak{c}$. If $\gamma_0 \in \mathfrak{c}$, we iterate one more time in Step 4 to replace γ_0 by γ_1 (that is, replacing N by $N + 1$). Indeed, by (1) γ_0 and γ_1 cannot both be in $\mathfrak{c}$. We can assume from now on that $\gamma_0 \notin \mathfrak{c}$. The group $U_+(E)$ acts on the set $\{\gamma_n, n \in \mathbb{Z}\}$; thus there exists an integer $P_0 \geq 1$ such that $\gamma_{n+P_0} = \epsilon_+\gamma_n$ for all $n \geq 0$. Therefore, for any $n \in \mathbb{Z}$ the union of the (disjoint) rational cones $RC_\mathfrak{m}(\gamma_n, \gamma_{n+1}; \mathfrak{a}), \ldots, RC_\mathfrak{m}(\gamma_{n+P-1}, \gamma_{n+P}; \mathfrak{a})$, with $P := i_\mathfrak{m}P_0$, gives a set of representatives of $\mathfrak{a} \cap E_\mathfrak{m}$ modulo $U_\mathfrak{m}(E)$ with generators in $\mathfrak{a}\mathfrak{f}$. However, although γ_0, and thus also γ_P, do not belong to $\mathfrak{c}$, it is possible that $\gamma_n \in \mathfrak{c}$ for some n in the range $1 \leq n \leq P - 1$. In that case, γ_{n-1} and γ_{n+1} do not lie in $\mathfrak{c}$, by (1), and we use in Step 6.1 the fact that $RC_\mathfrak{m}(\gamma_{n-1}, \gamma_n; \mathfrak{a}) \cup RC_\mathfrak{m}(\gamma_n, \gamma_{n+1}; \mathfrak{a}) = RC_\mathfrak{m}(\gamma_{n-1}, \gamma_{n+1}; \mathfrak{a})$ to get rid of cones with $\gamma_n \in \mathfrak{c}$. We end up with a rational cone decomposition having generators suitable for constructing a $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$ modulo $\mathfrak{m}$ using (5.9).

We will now estimate the complexity of the algorithm and the number of cones obtained at the end. First we find an upper bound on N, the number of iterations in Step 3. Assume $1 \leq t < N - 1$. Since $\tilde{\gamma}_{t+1}^{(1)} < \tilde{\gamma}_t^{(1)}$ and $\tilde{\gamma}_{t+1}^{(2)} < \tilde{\gamma}_t^{(2)}$ we have $\mathcal{N}(\tilde{\gamma}_{t+1}) < \mathcal{N}(\tilde{\gamma}_t)$, and since both are divisible by $\mathcal{N}(\mathfrak{a}\mathfrak{f})$ we have $N \leq \mathcal{N}(h)/\mathcal{N}(\mathfrak{a}\mathfrak{f}) + 1$. Now assume, without loss of generality, that $\sqrt{D_E}^{(1)} = \sqrt{D_E} > 0$ and $\sqrt{D_E}^{(2)} = -\sqrt{D_E} < 0$. Write $h = a + b\sqrt{D_E}$ with $a, b \in \frac{1}{2}\mathbb{Z}$. Since $h^{(2)} > h^{(1)}$, it follows that $b < 0$, and also $a > -b\sqrt{D_E} > 0$, as $h \in \mathbb{Z}_E^+$. On the other hand, $a < g - b\sqrt{D_E}$ because $h^{(1)} < g$. From the fact that $\mathfrak{a}\mathfrak{f} = \mathbb{Z}g + \mathbb{Z}h$, we find that $b = -\mathcal{N}(\mathfrak{a}\mathfrak{f})/2g$. We compute $\mathcal{N}(h) = a^2 - b^2D_E < (g - b\sqrt{D_E})^2 - b^2D_E = g^2 - 2gb\sqrt{D_E} = g^2 + \mathcal{N}(\mathfrak{a}\mathfrak{f})\sqrt{D_E} \in O(\mathcal{N}(\mathfrak{a}\mathfrak{f})^2\sqrt{D_E})$. Thus Step 3 requires $O(\mathcal{N}(\mathfrak{a}\mathfrak{f})\sqrt{D_E})$ operations in E.

Next we estimate the size of $P = i_\mathfrak{m}P_0$. By [19, p. 161] we have

$$\log C + \log \frac{\epsilon_+^{(2)}}{\epsilon_+^{(2)} - \epsilon_+^{(1)}} + \frac{1}{2}\log D_E \geq P\frac{\log \epsilon_+^{(2)}}{\epsilon_+^{(2)} - \epsilon_+^{(1)}} \tag{5.10}$$

where

$$C := \frac{\epsilon_\mathfrak{m}^{(2)} - \epsilon_\mathfrak{m}^{(1)}}{\sqrt{D_E}} \inf_{n\in\mathbb{Z}} \frac{\mathcal{N}(\gamma_n)}{\mathcal{N}(\mathfrak{a}\mathfrak{f})}.$$

For $n \in \mathbb{Z}$ we see that $b(\gamma_{n-1}, \gamma_n) = 2$ if and only if γ_n is midway between γ_{n-1} and γ_{n+1}, in which case we say γ_n is a *midpoint*. If γ_n is not a midpoint we say γ_n is a *vertex*. If γ_n is a vertex we have $\mathcal{N}(\gamma_n) \leq \mathcal{N}(\mathfrak{a}\mathfrak{f})\sqrt{D_E}$ (see [19, Prop. 5.5]) and it follows that $C \leq \epsilon_\mathfrak{m}^{(2)}$. Substitution in (5.10) gives

$$P \in O\big(\epsilon_+^{(2)}(\log \epsilon_\mathfrak{m}^{(2)} + \log D_E)\big) \subset \tilde{O}\big(i_\mathfrak{m}\epsilon_+^{(2)} \log D_E\big).$$

Lastly, we need to explain how to perform Step 6.2, we need to estimate the cost of the computation, and we need to estimate the number of points in the sets $PC_\mathfrak{m}(b_0, b_1; \mathfrak{a})$. There are two cases to consider, (I) $(b_0, b_1) = (\gamma_n, \gamma_{n+1})$ and (II) $(b_0, b_1) = (\gamma_n, \gamma_{n+2})$, for an arbitrary $n \in \mathbb{Z}$. We have the bijection

$$\mathfrak{a}/(\mathbb{Z}b_0 + \mathbb{Z}b_1) \xrightarrow{1:1} \{sb_0 + tb_1 \text{ with } s, t \in \mathbb{Q},\ 0 < s \leq 1,\ 0 \leq t < 1\} \cap \mathfrak{a},$$

defined as follows. For a given class $\bar{\alpha}$ in $\mathfrak{a}/(\mathbb{Z}b_0 + \mathbb{Z}b_1)$, lift $\bar{\alpha}$ to an arbitrary element $\alpha \in \mathfrak{a}$ and write $\alpha = sb_0 + tb_1$ with $s, t \in \mathbb{Q}$. Then the map above sends $\bar{\alpha}$ to

$$[\alpha]_{(b_0,b_1)} := (s - \lceil s \rceil + 1)b_0 + (t - \lfloor t \rfloor)b_1.$$

Moreover, since b_0 and b_1 lie in $\mathfrak{af}$ there is a well-defined map from $\mathfrak{a}/(\mathbb{Z}b_0+\mathbb{Z}b_1)$ to $\mathfrak{a}/\mathfrak{af}$ which sends $\bar\alpha$ to the class of α modulo $\mathfrak{af}$. The set $PC_{\mathfrak{m}}(b_0,b_1;\mathfrak{a})$ consists of precisely those elements $[\alpha]_{(b_0,b_1)}$ for which $\bar\alpha\in\mathfrak{a}/(\mathbb{Z}b_0+\mathbb{Z}b_1)$ is congruent to 1 modulo $\mathfrak{f}$. Since $\mathfrak{a}$ and $\mathfrak{f}$ are coprime this map is surjective and therefore $PC_{\mathfrak{m}}(b_0,b_1;\mathfrak{a})$ contains exactly $d/\mathcal{N}(\mathfrak{f})$ elements, where $d:=(\mathfrak{a}:\mathbb{Z}b_0+\mathbb{Z}b_1)$. Using the methods of [9, §4.1.3], two elements α_0 and α_1 of $\mathfrak{a}$ can be constructed with $\mathfrak{a}=\mathbb{Z}\alpha_0+\mathbb{Z}\alpha_1$ and $\mathfrak{a}/(\mathbb{Z}b_0+\mathbb{Z}b_1)=(\mathbb{Z}/d_0\mathbb{Z})\bar\alpha_0+(\mathbb{Z}/d_1\mathbb{Z})\bar\alpha_1$, where d_0 and d_1 are positive integers and $d:=d_0d_1$. Thus the elements of $\mathfrak{a}/(\mathbb{Z}b_0+\mathbb{Z}b_1)$ can easily be enumerated in $O(d)$ operations in E. For case (I) we have $\mathbb{Z}\gamma_n+\mathbb{Z}\gamma_{n+1}=\mathfrak{af}$ and therefore $d=\mathcal{N}(\mathfrak{f})$ and $PC_{\mathfrak{m}}(\gamma_n,\gamma_{n+1};\mathfrak{a})$ contains only one element. For case (II) we have

$$d=(\mathfrak{a}:\mathbb{Z}\gamma_n+\mathbb{Z}\gamma_{n+2})=(\mathfrak{a}:\mathbb{Z}\gamma_n+\mathbb{Z}\gamma_{n+1})(\mathbb{Z}\gamma_n+\mathbb{Z}\gamma_{n+1}:\mathbb{Z}\gamma_n+\mathbb{Z}\gamma_{n+2})=\mathcal{N}(\mathfrak{f})\,b(\gamma_n,\gamma_{n+1}).$$

If γ_{n+1} is a midpoint we have $b(\gamma_n,\gamma_{n+1})=2$. We now need to estimate the size of $b(\gamma_n,\gamma_{n+1})$ when γ_n is a vertex. Since $b(\gamma_n,\gamma_{n+1})=b(\gamma_{n+P_0},\gamma_{n+P_0+1})$ it is enough to look at what happens for the vertices among $\gamma_0,\ldots,\gamma_{P_0-1}$. Writing $b_n:=b(\gamma_{n-1},\gamma_n)$ to simplify the notation, we have by construction

$$\frac{\gamma_{n-1}^{(1)}}{b_n-1}>\gamma_n^{(1)}>\frac{\gamma_{n-1}^{(1)}}{b_n}$$

and therefore

$$\frac{\gamma_0^{(1)}}{(b_{P_0}-1)(b_{P_0-1}-1)\cdots(b_1-1)}>\gamma_{P_0}^{(1)}>\frac{\gamma_0^{(1)}}{b_{P_0}b_{P_0-1}\cdots b_1}.$$

From the fact that $\gamma_{P_0}=\epsilon_+\gamma_0$ we find that

$$\epsilon_+^{(2)}>\prod_{i=1}^{P_0}(b_i-1). \tag{5.11}$$

The indices i for which $b_i=2$, that is, corresponding to the midpoints, do not contribute to the product. For indices corresponding to vertices we get

$$\sum_{\substack{1\le i\le P_0\\ \gamma_i \text{ is a vertex}}} b_i\in O(\epsilon_+^{(2)}).$$

We now put everything together to get the result. For Step 1, we assume that an ideal is given by a 2×2 integral matrix expressing a basis of the ideal of the (fixed) integral basis of E. This step amounts to an HNF reduction of a 2×4 matrix (see [8, §4.7.1]). Since we can reduce the entries of this matrix modulo $\mathcal{N}(\mathfrak{af})$ this step takes $\tilde{O}(\log(\mathcal{N}(\mathfrak{af})))$ bit operations and hence is negligible. Step 3 takes $O(\mathcal{N}(\mathfrak{af})\sqrt{D_E})$ operations in E. The loop in Step 6 is iterated P times. The most costly operation is in Step 6.2. The cost of computing α_0, α_1, d_0, and d_1 is essentially that of an SNF reduction of a 2×2 matrix with coefficients of size $\le\mathcal{N}(\mathfrak{af})$ and hence can be neglected. Enumerating the elements of $PC_{\mathfrak{m}}(b_0,b_1;\mathfrak{a})$ takes a total of $O(\mathcal{N}(\mathfrak{f})P)$ operations in E for the midpoints and $O(i_{\mathfrak{m}}\mathcal{N}(\mathfrak{f})\epsilon_+)$ for the vertices. This gives the estimate on the complexity of the algorithm. To count the cones we observe that the midpoints give $O(P)$ cones and the vertices give $O(i_{\mathfrak{m}}\epsilon_+)$ cones. The conclusion is established by using the fact that $i_{\mathfrak{m}}\in O(\mathcal{N}(\mathfrak{f}))$. □

Remark 5.33. One could ask what would happen if we were first to construct a cone decomposition using the algorithm without any restriction related to $\mathfrak{c}$, that is, deleting Step 4 and always doing the first part in Step 6.1, then choosing the prime ideal $\mathfrak{c}$ so that the decomposition computed is $\mathfrak{c}$-admissible. In fact this would not change the complexity or even the order of the number of cones, since both are dominated by the contributions of the midpoints and, in fact, for these we get the same number of discrete cones in cases (I) and (II). On the other hand, this would probably force the norm of $\mathfrak{c}$ to get significantly larger and that would adversely affect the complexity of the remaining computations.

Remark 5.34. The complexity and the estimate of the number of cones given by this proposition appear in practice to be very pessimistic as they are of the order of the exponential of R_E, the regulator of E, whereas computations point towards something of the size of R_E. Indeed, one can use (5.11) to show that the number of vertices among $\gamma_0, \ldots, \gamma_{P_+}$ is $O(R_E)$. However, it appears difficult to bound the number of midpoints. One can prove that if γ_n is a vertex then the number of midpoints following it is $\lfloor 1/(1 - b_n + \gamma_{n-1}^{(1)}/\gamma_n^{(1)}) \rfloor$, and so this problem is related to the question of how close a quadratic irrationality can be to an integer. In order to bound more efficiently the number of cones one would need to bound the size of the b_n's. This could be done for example using (5.11) by finding some non-trivial lower bound on the number of vertices.

5.5. **Computations of p-adic L-functions.** We use the results from the preceding subsections to estimate the complexity of computing L-functions. We will make certain assumptions. As noted above, we assume we have computed the necessary data to work in E: ring of integers, class group, units, etc. We assume also that we have at our disposal a prime ideal $\mathfrak{c}$ satisfying the hypotheses (H1), (H2), and (H3) and the additional hypothesis

(H4) Either χ is non-trivial and $\chi(\mathfrak{c}) \neq 1$, or χ is trivial and $\langle c \rangle \notin 1 + p^{e+1}\mathbb{Z}_p$.[26]

We assume we have computed a list of integral ideals $\mathfrak{a}_i$, $i = 1, \ldots, h_\mathfrak{m}(E)$, coprime to $\mathfrak{c}$ and $\mathfrak{m}$ and representing all the classes of $\mathrm{Cl}_\mathfrak{m}(E)$. Finally, we assume we have computed a cone decomposition for each ideal $\mathfrak{a}_i$; we will denote by B the maximum number of cones among these decompositions (see the previous subsection). In what follows δ will denote the degree of $\mathbb{Q}_p(\chi)/\mathbb{Q}_p$.

Lemma 5.35. *Assume the ERH. Then there exists a prime ideal $\mathfrak{c}$ satisfying hypotheses* (H1) *through* (H4)*, with $c \in O(\log^2(\mathcal{N}(\mathfrak{f})D_E))$ if χ is non-trivial and $c \in O\tilde{~}(p^{2m_0}\log^2(D_E))$ if χ is trivial, where $m_0 \geq 0$ is such that $\mathbb{Q}_{m_0} = E \cap \mathbb{Q}_\infty$.*

Proof. We use Theorem 1 of of [2]. For the case χ non-trivial the application is direct. For the case χ trivial we apply the theorem to the character ρ generating the group of characters of $\mathrm{Gal}(E_1/E)$. The absolute norm of the conductor of ρ divides the absolute norm of the conductor of $\mathbb{Q}_{m_0+1}/\mathbb{Q}_{m_0}$, the p-adic valuation of which is $v_p(q) + (p^{m_0+1} - 1)/(p - 1)$. The result follows. □

Theorem 5.36. *Let M and N be positive integers. Under the assumptions enumerated at the beginning of this subsection the measures $\mu_{p,\mathfrak{m}}^{\mathfrak{a}_i,\mathfrak{c}}$, for $i = 1, \ldots, h_\mathfrak{m}(E)$, can be computed to the precision (p^M, T^N) in $O\tilde{~}(h_\mathfrak{m}(E)d^{d+3}BN^{d+1}Mc\log p)$ bit operations.*

Proof. This follows directly from Theorem 5.21. □

Corollary 5.37. *Let M be a positive integer and let $s \in \mathbb{Z}_p$, with $s \neq 1$ if χ is trivial. Under the assumptions enumerated at the beginning of this subsection and after precomputations of cost $O\tilde{~}(h_\mathfrak{m}(E)p^{d+1}d^{d+3}BM^{d+2}c)$ bit operations, two algebraic integers β and γ, both belonging to $\mathbb{Z}[\chi]$ and with $\gamma L_{p,\mathfrak{m}}(\chi; s)$ lying in $\mathbb{Z}_p[\chi]$ and $|\gamma L_{p,\mathfrak{m}}(\chi; s) - \beta|_p \leq p^{-M}$, can be computed in $O\tilde{~}(h_\mathfrak{m}(E)(p^2M^3 + \delta M\log p))$ bit operations. Moreover, $p^{-1/(p-1)} \leq |\gamma|_p \leq 1$ if χ is non-trivial and $|\gamma|_p = p^{-e}|s - 1|_p$ if χ is trivial.*

Proof. We precompute the measures $\mu_{p,\mathfrak{m}}^{\mathfrak{a}_i,\mathfrak{c}}$, for $i = 1, \ldots, h_\mathfrak{m}(E)$, to the precision (p^M, T^N), with $N := pM + 2$, the computation cost being given by Theorem 5.36. We let β be an approximation of the sum in (4.4) to the precision p^M. The values of $\mathcal{Z}_{p,\mathfrak{m}}(\mathfrak{a}_i^{-1}, \mathfrak{c}; s)$, for $i = 1, \ldots, h_\mathfrak{m}(E)$, to the precision p^M are computed using Corollary 5.23 *mutatis mutandis* in $O\tilde{~}(h_\mathfrak{m}(E)p^2M^3)$ operations. The rest of the computation of β takes $O(h_\mathfrak{m}(E)\delta M\log p)$ bit operations. We now let γ be an approximation of $\chi(\mathfrak{c})\langle c \rangle^{1-s} - 1$ to the precision p^M. The

[26] Note that we always have $\langle c \rangle \in 1 + p^e\mathbb{Z}_p$ by Lemma 4.3.

computation of γ takes $O\tilde{}(M^2\log^2 p + \delta M \log p)$ bit operations, and it follows from (4.4) that $\gamma L_{p,\mathfrak{m}}(\chi; s)$ lies in $\mathbb{Z}_p[\chi]$ and $|\gamma L_{p,\mathfrak{m}}(\chi; s) - \beta|_p \leq p^{-M}$. The assertions concerning the absolute value of γ are straightforward (see the proof of Corollary 4.16). □

Recall that $E \cap \mathbb{Q}_\infty = \mathbb{Q}_{m_0}$ and $E(\mathfrak{m}) \cap \mathbb{Q}_\infty = \mathbb{Q}_{m_0+m_1}$, so that $e = m_0 + v_p(q)$.

Theorem 5.38. *Let M and L be positive integers. Under the assumptions enumerated at the beginning of this subsection there exist polynomials $B(X)$ and $C(X)$ in $\mathbb{Z}_p[\chi][X]$, with a cost of $O\tilde{}(h_{\mathfrak{m}}(E)(p^{ed}d^{d+3}B(pM+L)^dM^2Lc + \delta M\log p))$ bit operations to compute, such that*

$$C(X)\mathfrak{I}_{p,\mathfrak{m}}(\chi; X) - B(X) \in \begin{cases} p^M\mathbb{Z}_p[\chi][[X]] + X^L\mathbb{Z}_p[\chi][[X]] & \text{if } \chi \text{ is trivial or not of type } W, \\ \dfrac{p^M}{X+\pi}\mathbb{Z}_p[\chi][[X]] + \dfrac{X^L}{X+\pi}\mathbb{Z}_p[\chi][[X]] & \text{otherwise,} \end{cases}$$

with $\pi \in \mathbb{O}_p$ satisfying

$$\frac{1}{p^{m_1-1}(p-1)} \leq v_p(\pi) \leq \frac{1}{p-1}.$$

Moreover, $p^{-1/(p-1)} \leq |C(0)|_p \leq 1$ if χ is non-trivial and $C(0) = 0$, $|C'(0)|_p = 1$ if χ is trivial.

Proof. We use the notation and results from the proof of Theorem 4.15. The polynomial $C(X)$ is an approximation modulo (p^M, X^L) of the power series $C(\mathfrak{c}, \chi; X)$ and the polynomial $B(X)$ is approximation modulo (p^M, X^L) of the power series

$$\sum_{i=1}^{h_{\mathfrak{m}}(E)} \chi(\mathfrak{a}_i^{-1})N(\mathfrak{a}_i; X)A(\mathfrak{a}_i, \mathfrak{c}; X).$$

The first assertion follows by (4.7) and the integral properties of $\mathfrak{I}_{p,\mathfrak{m}}(\chi; X)$, with $\pi := (\xi-1)/\xi$. Since ξ has order p^m for some integer m with $1 \leq m \leq m_1$ this proves the inequalities on the p-adic valuation of π. The properties of $C(X)$ follow from (H4). We now evaluate the complexity of the computation of $B(X)$ and $C(X)$. Let $\mathfrak{a}$ be one of the ideals $\mathfrak{a}_i$ and let $\{C_1, \dots, C_m\}$ be a $\mathfrak{c}$-admissible cone decomposition of $\mathfrak{a}$. Then

$$A(\mathfrak{a}, \mathfrak{c}; X) = \sum_{j=1}^{m} \mathfrak{I}_p(C_j, \mathfrak{c}; X)$$

and the computation cost of $A(\mathfrak{a}, \mathfrak{c}; X)$ to the precision (p^M, X^L) follows from Theorem 5.24. The computation time of $C(X)$ is negligible compared to that of $B(X)$. □

Corollary 5.39. *Let M be a positive integer and let $s \in \mathbb{Z}_p$, with $s \neq 1$ if χ is trivial. Under the assumptions enumerated at the beginning of this subsection and after precomputations costing $O\tilde{}(h_{\mathfrak{m}}(E)(p^{(e+1)d}d^{d+3}BM^{d+2}Lc + \delta M\log p))$ bit operations, two algebraic integers, β and γ, both belonging to $\mathbb{Z}[\chi]$ and with $\gamma L_{p,\mathfrak{m}}(\chi; s)$ lying in $\mathbb{Z}_p[\chi]$ and*

$$|\gamma L_{p,\mathfrak{m}}(\chi; s) - \beta|_p \leq \begin{cases} p^{-M} & \text{if } \chi \text{ is trivial or not of type } W, \\ p^{-M+1/(p-1)} & \text{otherwise,} \end{cases} \tag{5.12}$$

can be computed in $O\tilde{}(M^2\log p\,(\delta/e + \log p))$ bit operations. Moreover, $p^{-1/(p-1)} \leq |\gamma|_p \leq 1$ if χ is non-trivial and $|\gamma|_p = p^{-e}|s-1|_p$ if χ is trivial.

Proof. We precompute the polynomials $B(X)$ and $C(X)$ with $L := \lceil M/e \rceil$. The precomputation cost is given by Theorem 5.38. Then we compute $t := u^{1-s} - 1$ to the precision p^M in $O\tilde{}(M^2\log^2 p)$ bit operations, and compute β to be $B(t)$, respectively γ to be $C(t)$, to the precision p^M in $O\tilde{}(\delta M^2/e \log p)$ bit operations. The result follows from (4.6) and the theorem. □

We conclude with the cost of computing a single value of a p-adic L-function without precomputations.

Theorem 5.40. *Let M be a positive integer and let $s \in \mathbb{Z}_p$, with $s \neq 1$ if χ is trivial. Under the assumptions enumerated at the beginning of this subsection, two algebraic integers β and γ, both belonging to $\mathbb{Z}[\chi]$ and with $\gamma L_{p,\mathfrak{m}}(\chi; s)$ lying in $\mathbb{Z}_p[\chi]$ and $|\gamma L_{p,\mathfrak{m}}(\chi; s) - \beta|_p \leq p^{-M}$, can be computed at a cost of $O\tilde{}(h_{\mathfrak{m}}(E)(p^d d^{d+3} M^{d+2} c + \delta M \log p))$ bit operations. Moreover, $p^{-1/(p-1)} \leq |\gamma|_p \leq 1$ if χ is non-trivial and $|\gamma|_p = p^{-e}|s-1|_p$ if χ is trivial.*

Proof. We proceed as in the proof of Corollary 5.37 with the same definitions for β and γ. The cost of computing γ is the same. We construct β by computing the values of $\mathcal{Z}_{p,\mathfrak{m}}(\mathfrak{a}_i^{-1}, \mathfrak{c}; s)$, for $i = 1, \ldots, h_{\mathfrak{m}}(E)$, to the precision p^M, using Theorem 5.28 *mutatis mutandis.* The cost of this computation is $O\tilde{}(h_{\mathfrak{m}}(E)(p^d d^{d+3} M^{d+2} c + \delta M \log p))$ bit operations. The result follows. □

References

[1] Y. Amice. Interpolation p-adique. *Bull. Soc. Math. France*, 92:117–180, 1964.

[2] E. Bach. Explicit bounds for primality testing and related problems. *Math. Comp.*, 55(191):355–380, 1990.

[3] D. Barsky. Fonctions zeta p-adiques d'une classe de rayon des corps de nombres totalement réels. In *Groupe d'Etude d'Analyse Ultramétrique (5e année: 1977/78)*, pages Exp. No. 16, 23. Secrétariat Math., Paris, 1978.

[4] K. Belabas. Topics in computational algebraic number theory. *J. Théor. Nombres Bordeaux*, 16(1):19–63, 2004.

[5] A. Besser, P. Buckingham, R. de Jeu, and X.-F. Roblot. On the p-adic Beilinson conjecture for number fields. *Pure Appl. Math. Q.*, 5(1):375–434, 2009.

[6] P. Cartier and Y. Roy. Certains calculs numériques relatifs à l'interpolation p-adique des séries de Dirichlet. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 269–349. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[7] Pi. Cassou-Noguès. Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. *Invent. Math.*, 51(1):29–59, 1979.

[8] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[9] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[10] P. Colmez. Fonctions d'une variable p-adique. online notes available at `http://www.math.jussieu.fr/~colmez/fonctionsdunevariable.pdf`.

[11] P. Colmez. Résidu en $s = 1$ des fonctions zêta p-adiques. *Invent. Math.*, 91(2):371–389, 1988.

[12] P. Deligne and K. Ribet. Values of abelian L-functions at negative integers over totally real fields. *Invent. Math.*, 59(3):227–286, 1980.

[13] F. Diaz y Diaz and E. Friedman. Colmez cones for fundamental units of totally real cubic fields. preprint, 2011.

[14] F. Diaz y Diaz and E. Friedman. Signed Shintani-Colmez cones. preprint, 2011.

[15] J. S. Ellenberg, S. Jain, and A. Venkatesh. Modelling λ-invariants by p-adic Random Matrices. preprint, 2011.

[16] R. Ernvall and T. Metsänkylä. Computation of the zeros of p-adic L-functions. *Math. Comp.*, 58(198):815–830, S37–S53, 1992.

[17] R. Ernvall and T. Metsänkylä. Computation of the zeros of p-adic L-functions. II. *Math. Comp.*, 62(205):391–406, 1994.

[18] R. Greenberg. On p-adic Artin L-functions. *Nagoya Math. J.*, 89:77–87, 1983.

[19] D. Hayes. Brumer elements over a real quadratic base field. *Exposition. Math.*, 8(2):137–184, 1990.

[20] K. Iwasawa and C. Sims. Computation of invariants in the theory of cyclotomic fields. *J. Math. Soc. Japan*, 18:86–96, 1966.

[21] N. Katz. Another look at p-adic L-functions for totally real fields. *Math. Ann.*, 255(1):33–43, 1981.

[22] T. Kubota and H.-W. Leopoldt. Eine p-adische Theorie der Zetawerte. I. Einführung der p-adischen Dirichletschen L-Funktionen. *J. Reine Angew. Math.*, 214/215:328–339, 1964.

[23] S. Lang. *Cyclotomic fields I and II*, volume 121 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, seconde edition, 1990.

[24] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999.

[25] K. A. Ribet. Report on p-adic L-functions over totally real fields. In *Journées Arithmétiques de Luminy (Colloq. Internat. CNRS, Centre Univ. Luminy, Luminy, 1978)*, volume 61 of *Astérisque*, pages 177–192. Soc. Math. France, Paris, 1979.

[26] A. M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[27] X.-F. Roblot and D. Solomon. Verifying a p-adic abelian Stark conjecture at $s = 1$. *J. Number Theory*, 107(1):168–206, 2004.

[28] X.-F. Roblot and A. Weiss. Numerical evidence toward a 2-adic equivariant "Main Conjecture". *Experiment. Math.*, 20(2):169–176, 2011.

[29] T. Shintani. On evaluation of zeta functions of totally real algebraic number fields at non-positive integers. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 23(2):393–417, 1976.

[30] D. Solomon. The Shintani cocycle. II. Partial ζ-functions, cohomologous cocycles and p-adic interpolation. *J. Number Theory*, 75(1):53–108, 1999.

Université de Lyon, Université Lyon 1, CNRS UMR5208, Institut Camille Jordan, 43 blvd du 11 novembre 1918, 69622 Villeurbanne Cedex, France
E-mail address: roblot@math.univ-lyon1.fr

Tokyo Institute of Technology, Department of Mathematics, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8550, Japan
E-mail address: roblot@math.titech.ac.jp